日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

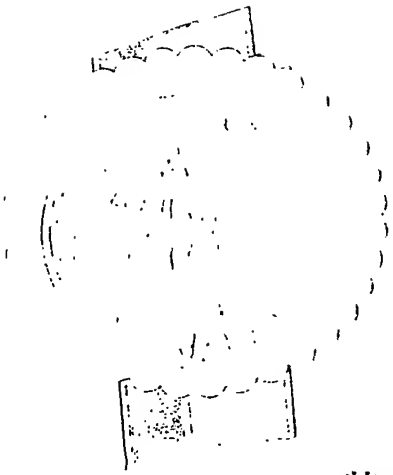
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　７月２５日

出願番号
Application Number: 特願２００２－２１６７５０

[ST. 10/C]: ［ＪＰ２００２－２１６７５０］

出願人
Applicant(s): 三洋電機株式会社
パイオニア株式会社
株式会社日立製作所
フェニックステクノロジーズ株式会社
富士通株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００３年　８月２８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７００５４

【書類名】　特許願

【整理番号】　1020333

【提出日】　平成14年 7月25日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 11/08

【発明者】

【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

【氏名】　堀　吉宏

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　多田　謙一郎

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　平井　達哉

【発明者】

【住所又は居所】　東京都千代田区丸の内１－３－１　東京銀行協会ビル１４Ｆ　フェニックステクノロジーズ株式会社内

【氏名】　津留　雅文

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【特許出願人】

【識別番号】　000001889

【住所又は居所】　大阪府守口市京阪本通２丁目５番５号

【氏名又は名称】　三洋電機株式会社

【特許出願人】

【識別番号】　000005016

【住所又は居所】　東京都目黒区目黒１丁目４番１号

【氏名又は名称】　パイオニア株式会社

【特許出願人】

【識別番号】　000005108

【住所又は居所】　東京都千代田区神田駿河台４丁目６番地

【氏名又は名称】　株式会社日立製作所

【特許出願人】

【識別番号】　300017636

【住所又は居所】　東京都千代田区丸の内１－３－１　東京銀行協会ビル１４Ｆ

【氏名又は名称】　フェニックステクノロジーズ株式会社

【特許出願人】

【識別番号】　000005223

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100064746

【弁理士】

【氏名又は名称】　深見　久郎

【選任した代理人】

【識別番号】　100085132

【弁理士】

【氏名又は名称】　森田　俊雄

【選任した代理人】

【識別番号】　100083703

【弁理士】

【氏名又は名称】　仲村　義平

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【選任した代理人】

【識別番号】　100098316

【弁理士】

【氏名又は名称】　野田　久登

【選任した代理人】

【識別番号】　100109162

【弁理士】

【氏名又は名称】　酒井　將行

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0006995

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ記憶装置

【特許請求の範囲】

【請求項１】　一定の手順に従って機密データの入出力を行ない、前記機密データを記憶し、かつ、前記一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置であって、

外部とデータの入出力を行なうインターフェースと、

複数の前記機密データを格納するデータ記憶部と、

前記機密データの入出力に関する複数の履歴情報を格納するログ記憶部と、

前記機密データの入出力を制御する制御部とを備え、

前記ログ記憶部は、それぞれ１つの前記履歴情報を格納する２つ以上の領域を循環的に利用するリングバッファとして設けられており、

前記ログ記憶部に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、

前記制御部は、前記機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報を前記インターフェースを介して受取り、前記ログ記憶部の複数の領域を所定の順序で検索して、前記ログ記憶部に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に前記受取った識別情報を含む前記機密データの入出力処理に対する履歴情報を新たに格納する、データ記憶装置。

【請求項２】　履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、

前記制御部は、入出力の対象となる機密データの識別情報を前記インタフェースを介して受取り、前記ログ記憶部の複数の領域を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、前記最新領域に格納されている履歴情報の一部または全てを前記インタフェースを介して出力する、請求項１に記載のデータ記憶装置。

【請求項３】　履歴情報の出力を伴う前記機密データの入力処理において、

前記制御部は、入出力の対象となる機密データの識別情報を前記インタフェー

スを介して受取り、前記ログ記憶部の複数の領域を所定の順序で検索して、前記最古領域と、前記受取った識別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの入力処理に対する新たな履歴情報として格納し、前記特定された最古領域に格納された履歴情報の一部または全てを前記インタフェースを介して出力する、請求項１に記載のデータ記憶装置。

【請求項４】　他の装置によって前記一定の手順の進行によって記録されたもう１つの履歴情報の入力を伴う前記機密データの再出力処理において、

前記制御部は、入出力の対象となる機密データの識別情報および前記もう１つの履歴情報とを前記インタフェースを介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納された履歴情報と、前記受取ったもう１つの履歴情報とに基づいて、前記機密データを出力するか否かを判定する、請求項２または請求項３に記載のデータ記憶装置。

【請求項５】　他の装置によって前記一定の手順の進行に従って記録されたもう１つの履歴情報の入力を伴う前記機密データの出力処理において、

前記制御部は、入出力の対象となる機密データの識別情報および前記もう１つの履歴情報を前記インタフェースを介して受取り、前記最古領域および前記最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって前記機密データの出力処理に対する新たな履歴情報として格納し、前記特定した最古領域に格納された履歴情報と、前記受取ったもう１つの履歴情報とに基づいて、前記機密データを出力するか否かを判定する、請求項２または請求項３に記載のデータ記憶装置。

【請求項６】　前記最古領域を特定した後、

前記制御部は、前記入出力処理における一定の手順が終了あるいは中止されるまでの間、前記特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する、請求項１から請求項５のいずれか１項に記載のデータ記憶装置。

【請求項７】　前記複数の履歴情報の各々は、前記ログ記憶部へ記憶された

順序を識別するための管理番号をさらに含み、

前記管理番号は、前記ログ記憶部に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号に基づいて、古い履歴情報が格納される前記最古領域を検出する、請求項１から請求項６のいずれか１項に記載のデータ記憶装置。

【請求項８】　前記ログ記憶部は、Ｎ（Ｎは２以上の自然数）個の領域を循環的に利用するリングバッファからなり、

前記管理番号は、Ｍ（Ｍは、Ｎ＜Ｍを満たす自然数）の剰余系からなる、請求項７に記載のデータ記憶装置。

【請求項９】　前記制御部は、前記ログ記憶部に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号を取得し、その取得した２つの管理番号の差に基づいて、２つの当該管理番号を含む２つの履歴情報が連続して格納されたか否かを判定し、２つの履歴情報が不連続に格納された履歴情報であるとき、前記連続する２つの領域のうち、後続領域を前記最古領域として検出する、請求項８に記載のデータ記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンスを記憶するデータ記憶装置に関し、特に、マルチアクセスが可能なデータ記憶装置においてコピーされた情報に対する著作権保護を可能とするデータ記憶装置に関するものである。

【０００２】

【従来の技術】

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００７】

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【０００８】

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカー

ドの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）、ライセンスを識別するためのライセンスＩＤ、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築し、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

【０００９】

メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。最終的に、携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

【００１０】

また、メモリカードは、他のメモリカードとの間でライセンスの移動または複製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンスに含まれる制御情報に従って決定される。

【００１１】

さらに、送受信中の不慮の中断によってライセンスが消失した場合に、その処理を再開でき、かつ、ライセンスの重複送信を防ぐためにライセンスの入出力に

関する直近の履歴情報を記録し、必要に応じて出力する機能をメモリカードは備えている。送信元である配信サーバあるいはメモリカードは、送信先のメモリカードから履歴情報を取得して、この履歴情報に従ってライセンスの送受信の再開を判断する。履歴情報は、ライセンスＩＤと送受信を示すステータス情報を含んでいる。

【００１２】

このように、携帯電話機のユーザは、携帯電話網を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。また、著作権者の権利を保護することができる。

【００１３】

【発明が解決しようとする課題】

しかし、従来のメモリカードにおいては、直近の履歴情報を保持するのみで、中断後、他のライセンスに対する送受信を行った場合に先の中断に対する履歴情報が消えてしまう。このような場合、複数の履歴情報を格納することにより、ユーザの利便性を改善することが可能である。

【００１４】

また、記憶素子に対するアクセスの高速化や、記憶素子の大容量化に伴い、複数のライセンスの送受信を並行して行なう要求が発生することが、今後、予想される。その場合、少なくとも並行して行われる処理に関する履歴情報を格納できるようにする必要性が生ずる。

【００１５】

このように、複数の履歴情報を格納できるようにする場合に、ライセンスの受信後に、該ライセンスを他のメモリカードに対して移したとすると、同一のライセンスＩＤに対して異なったステータスを持つ履歴情報が格納されるという問題が生じる。

【００１６】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開

可能とするための履歴情報を重複することなく複数格納できるデータ記憶装置を提供することである。

【００１７】

【課題を解決するための手段】

この発明によれば、データ記憶装置は、一定の手順に従って機密データの入出力を行ない、機密データを記憶し、かつ、一定の手順の進行に従って履歴情報を格納あるいは当該履歴情報を随時更新するデータ記憶装置であって、外部とデータの入出力を行なうインターフェースと、複数の機密データを格納するデータ記憶部と、機密データの入出力に関する複数の履歴情報を格納するログ記憶部と、機密データの入出力を制御する制御部とを備え、ログ記憶部は、それぞれ１つの履歴情報を格納する２つ以上の領域を循環的に利用するリングバッファとして設けられており、ログ記憶部に記憶される複数の履歴情報の各々は、当該履歴情報を記憶した入出力対象の機密データを識別する識別情報を含み、制御部は、機密データの入出力の処理が開始されたことに伴い入出力の対象となった機密データを識別する識別情報をインターフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、ログ記憶部に格納されている最も古い履歴情報を格納する領域を最古領域として特定し、その特定した最古領域に受取った識別情報を含む機密データの入出力処理に対する履歴情報を新たに格納する。

【００１８】

好ましくは、履歴情報の出力要求に対して履歴情報の一部または全てを出力する履歴情報の出力処理において、制御部は、入出力の対象となる機密データの識別情報をインタフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識別情報を含む最も新しい履歴情報を格納する領域を最新領域として特定し、最新領域に格納されている履歴情報の一部または全てをインタフェースを介して出力する。

【００１９】

好ましくは、履歴情報の出力を伴う前記機密データの入力処理において、制御部は、入出力の対象となる機密データの識別情報をインタフェースを介して受取り、ログ記憶部の複数の領域を所定の順序で検索して、最古領域と、受取った識

別情報を含む最も新しい履歴情報を格納する最新領域とを特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの入力処理に対する新たな履歴情報として格納し、特定された最古領域に格納された履歴情報の一部または全てをインタフェースを介して出力する。

【００２０】

好ましくは、他の装置によって一定の手順の進行によって記録されたもう１つの履歴情報の入力を伴う機密データの再出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう１つの履歴情報とをインタフェースを介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納された履歴情報と、受取ったもう１つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

【００２１】

好ましくは、他の装置によって一定の手順の進行に従って記録されたもう１つの履歴情報の入力を伴う機密データの出力処理において、制御部は、入出力の対象となる機密データの識別情報およびもう１つの履歴情報をインタフェースを介して受取り、最古領域および最新領域を特定し、その特定した最新領域に格納されている履歴情報の一部または全てを、特定した最古領域に複製することによって機密データの出力処理に対する新たな履歴情報として格納し、特定した最古領域に格納された履歴情報と、受取ったもう１つの履歴情報とに基づいて、機密データを出力するか否かを判定する。

【００２２】

好ましくは、最古領域を特定した後、制御部は、入出力処理における一定の手順が終了あるいは中止されるまでの間、特定された最古領域に格納された履歴情報を、当該手順の進行に従って随時更新する。

【００２３】

好ましくは、複数の履歴情報の各々は、ログ記憶部へ記憶された順序を識別するための管理番号をさらに含み、管理番号は、ログ記憶部に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号に基づいて、

古い履歴情報が格納される最古領域を検出する。

【００２４】

好ましくは、ログ記憶部は、Ｎ（Ｎは２以上の自然数）個の領域を循環的に利用するリングバッファからなり、管理番号は、Ｍ（Ｍは、Ｎ＜Ｍを満たす自然数）の剰余系からなる。

【００２５】

好ましくは、制御部は、ログ記憶部に連続して配置された２つの領域に格納された２つの履歴情報に含まれる各々の管理番号を取得し、その取得した２つの管理番号の差に基づいて、２つの当該管理番号を含む２つの履歴情報が連続して格納されたか否かを判定し、２つの履歴情報が不連続に格納された履歴情報であるとき、連続する２つの領域のうち、後続領域を最古領域として検出する。

【００２６】

したがって、この発明によれば、ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための複数の履歴情報を重複することなく格納できる。

【００２７】

【発明の実施の形態】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２８】

［実施の形態１］

図１は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００２９】

なお、以下では、デジタル放送網により配信された映像データを端末装置１０により受信して端末装置１０に装着されたデータ記憶装置であるＨＤ（ハードディスクドライブ）２０に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク３０に端末装置１０と接続されるライセン

ス提供装置４０からネットワーク３０を介してから受信してＨＤ２０に格納し、暗号化された映像データを端末装置１０に内蔵された専用の再生回路（図示せず）にて再生するデータ配信システムの構成を例にとって説明する。一方、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様で、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモリカードなどにおいても適用することが可能である。

【００３０】

図１を参照して、端末装置１０は、デジタル放送網により配信される、暗号化された映像データ（以下、コンテンツデータとも呼ぶ）をアンテナ１１を介して受信し、ＨＤ２０に記憶する。暗号化されたコンテンツデータ（以下、暗号化コンテンツデータとも呼ぶ）を復号するためのコンテンツ鍵を含むライセンスを管理し、かつ、配信するライセンス提供装置４０は、ライセンスの配信を求めてアクセスしてきた端末装置１０に装着されたＨＤ２０が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、ＨＤ２０が正当なデータ記憶装置であった場合のみ、端末装置１０に対してＨＤ２０においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置１０は、ネットワーク３０に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着されたＨＤ２０へ送信する。

【００３１】

図１においては、たとえば、ＨＤ２０は、端末装置１０に着脱可能な構成となっている。端末装置１０に装着されたＨＤ２０は、端末装置１０により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえでＨＤ２０内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコンテンツ鍵と暗号化コンテンツデータとを端末装置１０に与える。

【００３２】

そして、端末装置１０のユーザは、端末装置１０においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

【００３３】

このような構成とすることで、端末装置１０のユーザは、ライセンス管理機能を備えた正規の認証データを有するＨＤ２０を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

【００３４】

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、ライセンスを管理するライセンス提供装置４０であってもよいし、インターネットなどの通信網を介して接続されるライセンス提供装置４０とは別の配信サーバであってもよい。また、他のユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

【００３５】

したがって、本発明の実施の形態においては、ＨＤ２０、端末装置１０およびライセンス提供装置４０のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理中に異常が発生したときに、ライセンスが重複して存在することがないように、再処理の必要なライセンスを特定することでコンテンツデータの著作権保護を実現しつつ、不慮の送受信処理の異常終了から回復可能なシステムの構成について説明する。

【００３６】

図２は、図１に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

【００３７】

データＤｃは、コンテンツデータであって、ここでは映像データである。データＤｃは、コンテンツ鍵Ｋｃで復号可能な暗号化が施される。コンテンツ鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）が、この形式でデジタル放送網により端末装置１０のユーザに配布される。

【００３８】

なお、以下においては、Ｅ（Ｘ，Ｙ）という表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。また、データＤｃに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｉが配布される。

【００３９】

また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスＩＤ（ＬＩＤ）が端末装置１０を介してライセンス提供装置４０とＨＤ２０との間でやり取りされる。さらに、ライセンスとしては、データＤｃおよびコンテンツ鍵Ｋｃを識別するためのコードであるデータＩＤ（ＤＩＤ）や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ＡＣが存在する。

【００４０】

コンテンツ鍵Ｋｃと、制御情報ＡＣと、ＤＩＤと、ＬＩＤとを併せて、以後、ライセンスＬＩＣと総称することとする。ＤＩＤは、データＤｃとコンテンツ鍵Ｋｃとの対に対して割り当てられた識別情報、すなわち、暗号化データＥ（Ｋｃ，Ｄｃ）を識別するための識別情報となる。ＤＩＤは、ライセンスＬＩＣの他に、暗号化データＥ（Ｋｃ，Ｄｃ）とともに常に扱われる付加情報Ｄｉにも含まれ、参照できるようになっている。

【００４１】

図３は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００４２】

ＨＤ２０などのデータ記憶装置および端末装置１０などに備えられる再生回路には、固有のクラス公開鍵ＫＰｃｍｙおよびＫＰｃｐｙがそれぞれ設けられ、クラス公開鍵ＫＰｃｍｙおよびＫＰｃｐｙは、データ記憶装置に固有のクラス秘密鍵Ｋｃｍｙおよび再生回路に固有のクラス秘密鍵Ｋｃｐｙによってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密鍵を共有する単位をクラスと称する。記号「ｙ」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００４３】

また、データ記憶装置のクラス証明書としてＣｍｙが設けられ、再生回路のクラス証明書としてＣｐｙが設けられる。これらのクラス証明書は、データ記憶装置および再生回路のクラスごとに異なる情報を有する。

【００４４】

データ記憶装置のクラス証明書Ｃｍｙは、ＫＰｃｍｙ／／Ｉｃｍｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書Ｃｐｙは、ＫＰｃｐｙ／／Ｉｃｐｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐｙ／／Ｉｃｐｙ））の形式で出荷時に再生回路に記憶される。ここで、Ｘ／／Ｙは、ＸとＹとの連結を表わし、Ｈ（Ｘ）は、ハッシュ関数により演算されたデータＸのハッシュ値を表わす。マスタ鍵Ｋａは、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局によって安全に管理運用される。また、クラス情報Ｉｃｍｙ，Ｉｃｐｙは、クラスごとの機器に関する情報およびクラス公開鍵を含む情報データである。

【００４５】

また、Ｅ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））およびＥ（Ｋａ，Ｈ（ＫＰｃｐｙ／／Ｉｃｐｙ））は、それぞれＫＰｃｍｙ／／ＩｃｍｙおよびＫＰｃｐｙ／／Ｉｃｐｙに対する電子署名を行なった署名データである。

【００４６】

なお、認証局は、署名データを作成する公的な第三者機関であり、署名データＥ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））およびＥ（Ｋａ，Ｈ（ＫＰｃｐｙ／／Ｉｃｐｙ））は、認証局によって生成される。

【００４７】

さらに、データ記憶装置に対して安全かつ確実にライセンスＬＩＣを送信するための鍵として、データ記憶装置という媒体ごとに設定される個別公開鍵ＫＰｏｍｚと、個別公開鍵ＫＰｏｍｚで暗号化されたデータを復号することが可能な個別秘密鍵Ｋｏｍｚとが存在する。ここで、記号「ｚ」は、データ記憶装置を個別に識別するための識別子である。

【００４８】

データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置４０、データ記憶装置（ＨＤ２０）、および端末装置１０の再生回路において生成されるセッション鍵Ｋｓ１ｘ，Ｋｓ２ｘが用いられる。

【００４９】

ここで、セッション鍵Ｋｓ１ｘ，Ｋｓ２ｘは、ライセンス提供装置４０、データ記憶装置（ＨＤ２０）、もしくは端末装置１０の再生回路間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。「セッション」には、ライセンス提供装置４０からデータ記憶装置（ＨＤ２０）へライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置（ＨＤ２０）から端末装置１０の再生回路へライセンスを出力する「再生許諾セッション」がある。

【００５０】

これらのセッション鍵Ｋｓ１ｘ，Ｋｓ２ｘは、各セッションごとに固有の値を有することにより、ライセンス提供装置４０、データ記憶装置（ＨＤ２０）、および端末装置１０の再生回路によって管理される。具体的には、セッション鍵Ｋｓ１ｘは、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵Ｋｓ２ｘは、ライセンスの受信側によってセッションごとに発生される。なお、記号「ｘ」は、セッションにおける一連の処理

を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンスＬＩＣ、またはコンテンツ鍵を含むライセンスＬＩＣの一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００５１】

図４は、図１に示したライセンス提供装置４０の構成を示す概略ブロック図である。

【００５２】

ライセンス提供装置４０は、管理対象のライセンスを保持するデータベースであるコンテンツＤＢ４０２と、ライセンスを配信する配信セッションにおける全ての通信記録を随時記憶し、保持するデータベースであるログＤＢ４０４と、コンテンツＤＢ４０２およびログＤＢ４０４とバスＢＳ１を介してデータをやり取りし、所定の処理を行なうためのデータ処理部４１０と、ネットワーク３０を介して端末装置１０とデータ処理部４１０との間でデータ授受を行なうための通信装置４５０とを備える。

【００５３】

データ処理部４１０は、バスＢＳ１上のデータに応じて、データ処理部４１０の動作を制御するための配信制御部４１２と、配信制御部４１２により制御されて、配信セッション時にセッション鍵Ｋｓ１ｘを発生するためのセッション鍵発生部４１４と、端末装置１０から送られてくるＨＤ２０のクラス証明書Ｃｍｙに含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））を復号するためのＨＤ２０の認証鍵ＫＰａを保持するＫＰａ保持部４１６と、ＨＤ２０から送られてきたクラス証明書Ｃｍｙを通信装置４５０およびバスＢＳ１を介して受け、ＫＰａ保持部４１６から受ける認証鍵ＫＰａによって復号処理を行ない、クラス証明書Ｃｍｙに含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））の復号処理と、クラス証明書Ｃｍｙに含まれるＫＰｃｍｙ／／Ｉｃｍｙのハッシュ値の計算を行ない、両者の結果を比較チェックしてクラス証明書Ｃｍｙの検証を行なう認証部４１８と、配信セッションごとに、セッション鍵発生部４１４に

より生成されたセッション鍵Ｋｓ１ｘを認証部４１８によってクラス証明書Ｃｍｙから抽出したクラス公開鍵ＫＰｃｍｙを用いて暗号化し、バスＢＳ１に出力するための暗号処理部４２０と、セッション鍵Ｋｓ１ｘによって暗号化された上で送信されたデータをバスＢＳ１より受け、復号処理を行なう復号処理部４２２とを含む。

【００５４】

データ処理部４１０は、さらに、配信制御部４１２から与えられるライセンスＬＩＣを、復号処理部４２２によって得られたデータ記憶装置ごとに固有な個別公開鍵ＫＰｏｍｚによって暗号化するための暗号処理部４２４と、暗号処理部４２４の出力を、復号処理部４２２から与えられるセッション鍵Ｋｓ２ｘによってさらに暗号化してバスＢＳ１に出力するための暗号処理部４２６とを含む。

【００５５】

なお、個別公開鍵ＫＰｏｍｚおよびセッション鍵Ｋｓ２ｘは、セッション鍵Ｋｓ１ｘによって暗号化されたうえで端末装置１０から提供される。復号処理部４２２は、これを復号して個別公開鍵ＫＰｏｍｚを得る。

【００５６】

ライセンス提供装置４０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００５７】

図５は、図１に示した端末装置１０の構成を説明するための概略ブロック図である。

【００５８】

端末装置１０は、デジタル放送網によって伝送される信号を受信するアンテナ１０２と、アンテナ１０２からの信号を復調してデータに変換、あるいはアンテナ１０２から送信するデータを変調してアンテナ１０２に与える受信部１０４と、端末装置１０をネットワーク３０に接続するモデム１０６と、端末装置１０の各部のデータ授受を行なうバスB.Ｓ２と、バスＢＳ２を介して端末装置１０の動作を制御するコントローラ１０８と、ＨＤ２０とバスＢＳ２との間のデータの授受を制御するＨＤインターフェース部１１０とを含む。

【００５９】

端末装置１０は、さらに、上述したクラス証明書Ｃｐｙを保持する認証データ保持部１５０２を含む。ここで、端末装置１０のクラスを識別する識別子ｙは、ｙ＝３であるとする。

【００６０】

端末装置１０は、さらに、クラス固有の復号鍵であるクラス秘密鍵Ｋｃｐ３を保持するＫｃｐ保持部１５０４と、バスＢＳ２から受けたデータをクラス秘密鍵Ｋｃｐ３によって復号し、ＨＤ２０によって発生されたセッション鍵Ｋｓ１ｘを得る復号処理部１５０６とを含む。

【００６１】

端末装置１０は、さらに、ＨＤ２０に記憶されたコンテンツデータの再生を行なう再生許諾セッションにおいて、ＨＤ２０との間でやり取りされるデータを暗号化するためのセッション鍵Ｋｓ２ｘを乱数等により発生するセッション鍵発生部１５０８と、ＨＤ２０からコンテンツ鍵Ｋｃを受取る際に、セッション鍵発生部１５０８により発生されたセッション鍵Ｋｓ２ｘを復号処理部１５０６によって得られたセッション鍵Ｋｓ１ｘによって暗号化し、バスＢＳ２に出力する暗号処理部１５１０と、バスＢＳ２上のデータをセッション鍵Ｋｓ２ｘによって復号して、コンテンツ鍵Ｋｃを出力する復号処理部１５１２と、バスＢＳ２より暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を受けて、復号処理部１５１２からのコンテンツ鍵Ｋｃによって暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号してデータＤｃを再生部１５１６へ出力する復号処理部１５１４と、復号処理部１５１４からの出力を受けてコンテンツを再生するための再生部１５１６と、再生部１５１６の出力をデジタル信号からアナログ信号に変換するＤＡ変換部１５１８と、ＤＡ変換部１５１８の出力をテレビモニターなどの外部出力装置（図示省略）へ出力するための端子１５２０とを含む。

【００６２】

なお、図５においては、点線で囲んだ領域は暗号化コンテンツデータを復号して映像データを再生する専用回路である再生回路１５０を構成する。再生回路１５０は、セキュリティを向上させるために１チップ構成の半導体デバイスである

ことが好ましい。さらには、再生回路１５０は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

【００６３】

端末装置１０の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００６４】

ここでは、端末装置１０は、暗号化コンテンツデータを受信する機能、ライセンスの配信を受ける機能、再生許諾によって暗号化コンテンツデータを再生する機能を備えていたが、ＨＤ２０が端末装置１０から脱着可能なデータ記憶装置であることから明らかなように、これらの機能を別々の装置によって実現してもよい。この場合、目的とする機能を実現する装置にＨＤ２０を装着することで容易に実現できる。

【００６５】

図６は、図１に示すＨＤ２０の構成を説明するための概略ブロック図である。

すでに説明したように、データ記憶装置であるＨＤ２０には、クラス公開鍵ＫＰｃｍｙとクラス秘密鍵Ｋｃｍｙのペア、および個別公開鍵ＫＰｏｍｚと個別秘密鍵Ｋｏｍｚのペアが設けられるが、ＨＤ２０においては、これらを識別する識別子ｙ＝１、識別子ｚ＝２で表されるものとする。

【００６６】

したがって、ＨＤ２０は、クラス証明書Ｃｍ１として認証データＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を保持する認証データ保持部２０２と、クラス秘密鍵Ｋｃｍ１を保持するＫｃｍ保持部２０４と、個別秘密鍵Ｋｏｍ２を保持するＫｏｍ保持部２０６と、個別秘密鍵Ｋｏｍ２によって復号可能な個別公開鍵ＫＰｏｍ２を保持するＫＰｏｍ保持部２０８とを含む。

【００６７】

このように、データ記憶装置（ここではＨＤ２０）の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をデータ記憶装置単位で実行することが可能になる。

【００６８】

ＨＤ２０は、さらに、端末装置１０のＨＤインターフェース部１１０と端子２１０を介して信号を授受するＡＴＡ（ＡＴ－Ａｔｔａｃｈｍｅｎｔ）インターフェース部２１２と、ＨＤ２０におけるデータ伝送路であるバスＢＳ３と、ＡＴＡインターフェース部２１２からコントローラ２１４を介してバスＢＳ３に出力されたデータを、Ｋｏｍ保持部２０６により与えられた個別秘密鍵Ｋｏｍ２により復号し、ライセンス提供装置４０から配信されたライセンスＬＩＣをセキュアデータ記憶部２５０へ出力する復号処理部２１６と、ＫＰａ保持部２１８から認証鍵ＫＰａを受け、バスＢＳ３に出力されたデータの認証鍵ＫＰａによる復号処理を実行して復号結果をコントローラ２１４へ出力し、かつ、得られたクラス公開鍵ＫＰｃｍ１を暗号処理部２２２へ出力する認証部２２０と、切換スイッチ２６０によって選択的に与えられるセッション鍵Ｋｓ１ｘまたは Ｋｓ２ｘによって、切換スイッチ２６２によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号処理部２２４とを含む。

【００６９】

ＨＤ２０は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵Ｋｓ１ｘ，Ｋｓ２ｘを発生するセッション鍵発生部２２６と、セッション鍵発生部２２６の出力したセッション鍵Ｋｓ１ｘを認証部２２０によって得られる端末装置１０の再生回路１５０のクラス公開鍵ＫＰｃｐｙあるいは他のデータ記憶装置（ＨＤ２１とする）のクラス公開鍵ＫＰｃｍｙによって暗号化してバスＢＳ３に送出する暗号処理部２２２と、バスＢＳ３よりセッション鍵Ｋｓ２ｘによって暗号化されたデータを受けてセッション鍵発生部２２６より得たセッション鍵Ｋｓ１ｘまたは Ｋｓ２ｘによって復号する復号処理部２２８とを含む。

【００７０】

ＨＤ２０は、さらに、バスＢＳ３上のデータをクラス公開鍵ＫＰｃｍ１と対をなすクラス秘密鍵Ｋｃｍ１によって復号するための復号処理部２３０と、ライセンスＬＩＣをＨＤ２０からＨＤ２１へ移動または複製するために出力する際に、提供先のＨＤ２１から受信した個別公開鍵ＫＰｏｍｚ（ｚ≠２）によりライセンスＬＩＣを暗号化する暗号処理部２３２とを含む。

【００７１】

ＨＤ２０は、さらに、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を再生するためのライセンスＬＩＣと、ＨＤ２０が処理しているセッションの処理記録であるログとをバスＢＳ３より受けて記憶するセキュアデータ記憶部２５０を含む。そして、ライセンスＬＩＣは、セキュアデータ記憶部２５０内のセキュアデータ記憶部２５０に格納され、ログは、セキュアデータ記憶部２５０内のログメモリ２５３に格納される。セキュアデータ記憶部２５０は、たとえば半導体メモリによって構成される。

【００７２】

図７は、セキュアデータ記憶部２５０におけるメモリ構成を示した図である。

図７を参照して、セキュアデータ記憶部２５０は、ライセンス領域２５１と、有効フラグ領域２５２と、ログメモリ２５３とを含む。

【００７３】

ライセンス領域２５１は、Ｌ個（Ｌは自然数）の領域２５１１～２５１Ｌから成り、それぞれ１つのライセンス（コンテンツ鍵Ｋｃ、制御情報ＡＣ、ライセンスＩＤ（ＬＩＤ）、データＩＤ（ＤＩＤ））を格納する。

【００７４】

領域２５１１～２５１Ｌに格納された複数のライセンスの各々は、アドレス（以下、ＬＢＡ：Ｌｏｇｉｃａｌ　Ｂｌｏｃｋ　Ａｄｄｒｅｓｓと称する。）によって管理される。そして、各セッションにおいて記憶あるいは読出されるライセンスＬＩＣは、全てＬＢＡにより特定される。

【００７５】

領域２５１１～２５１Ｌに対応してｍａｘＬＢＡ＋１～ｍａｘＬＢＡ＋ＬのＬＢＡが付与されているものとする。たとえば、領域２５１３に格納されたライセンスＬＩＣは、ＬＢＡ：ｍａｘＬＢＡ＋３によって特定される。このとき、ＬＢＡ：０～ｍａｘＬＢＡは、ノーマルデータ記憶領域２７０に割当てられるものとする。詳細は後述する。

【００７６】

なお、ライセンス領域２５１には、ノーマルデータ記憶領域２７０に割当てら

れたＬＢＡ（０～ｍａｘＬＢＡ）に続く値、すなわち、ｍａｘＬＢＡ＋１～ｍａｘＬＢＡ＋ＬがＬＢＡとして割当てられると説明したが、ライセンス領域２５１に割当てるＬＢＡを限定するものではない。ライセンス領域２５１に割当てたＬ個のＬＢＡによって、それぞれが領域２５１１～２５１Ｌのいずれか１つを指定できる値であればいかなる値であってもよく、ノーマルデータ記憶領域２７０に割当てたＬＢＡと重複する値、あるいは、独立した値をＬＢＡとして割当ててもよい。

【００７７】

また、有効フラグ領域２５２は、セキュアデータ記憶部２５０上の記憶位置を特定するＬＢＡそれぞれに対応して設けられ、対応するＬＢＡによって特定される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

【００７８】

有効フラグ領域２５２は、領域２５２１～２５２Ｌから成り、領域２５２１～２５２Ｌは、それぞれ、対応する領域２５１１～２５１Ｌに格納されたライセンスＬＩＣの”有効”、または”無効”を格納する。

【００７９】

有効フラグ領域２５２のフラグが”有効”であるとき、フラグに対応するＬＢＡによって特定されるセキュアデータ記憶部２５０上の記憶位置に記憶されているライセンスＬＩＣは利用可能であり、ユーザはそのライセンスＬＩＣ内のコンテンツ鍵Ｋｃを再生許諾によって読出して、対応する暗号化コンテンツデータを復号し、コンテンツデータを再生したり、そのライセンスＬＩＣを他のデータ記憶装置に移動・複製することができる。

【００８０】

一方、有効フラグ領域２５２のフラグが”無効”であるとき、そのフラグに対応するＬＢＡによって特定されるセキュアデータ記憶部２５０上の記憶位置に記憶されているライセンスＬＩＣは利用不可であり、ＨＤ２０のコントローラ２１４によって、そのＬＢＡからのライセンスＬＩＣは拒否される。すなわち、消去されたのと同じ状態である。したがって、ユーザはそのライセンスＬＩＣに対応したコンテンツデータを再生することはできない。この有効フラグ領域２５２の

フラグは、ライセンスの新たな記憶によって”有効”とされ、ライセンスの移動によって”無効”とされる。

【００８１】

ログメモリ２５３は、ライセンスをＨＤ２０に入出力する場合の履歴情報（以下では「ログ」と呼ぶ。）を１つ格納するＮ（Ｎは自然数）個の領域２５３１～２５３Ｎからなるリングメモリである。領域２５３１～２５３Ｎは、それぞれ、バンク０～Ｎ－１と称される領域を特定する名称が付与されている。したがって、バンクｎ（ｎはＮの剰余系）とは、ログメモリ上の領域２５３（ｎ－１）を示す。

【００８２】

ログメモリ２５３は、複数のログをリング状に格納する。すなわち、ログメモリ２５３は、バンク０によって特定される領域２５３１からログの格納を開始し、バンクＮ－１によって特定される領域２５３Ｎにログを格納すると、再びバンク０によって特定される領域２５３１に戻り、ログを格納する。

【００８３】

バンク０～Ｎ－１、すなわち、ログメモリ２５３の領域２５３１～２５３Ｎの各々に格納されるログは、管理番号領域２５４１と、ライセンスＩＤ（ＬＩＤ）領域２５４２と、Ｋｓ２ｘ領域２５４３と、ＳＴ１領域２５４４と、ＳＴ２領域２５４５と、ＫＰｃｍｙ領域２５４６と、ＬＢＡ領域２５４７とを含む。

【００８４】

管理番号領域２５４１は、ログをバンク０～Ｎ－１の各々に格納する際に、ログの格納の順序を示す管理番号を格納する。そして、管理番号は、Ｍ（Ｍ＞Ｎ、Ｍは自然数）の剰余系をなして、昇順に付与される。この管理番号を格納することによって、最新のログを格納した、あるいは、最も古いログを格納したバンクを検索することができるようになる。すなわち、最初に管理番号１のログがバンク０に格納されるとすると、そのログの管理番号領域２５４１は、管理番号”１”を格納する。そして、ライセンスの入出力に伴い、新たなログを格納するごとに、バンク２から順に使用し、そのログの管理番号領域２５４１に、新たなログを格納するバンクの直前のバンクに格納される最新のログの管理番号領域２５４

１に格納される管理番号に１づつ増加した管理番号を格納する。したがって、各バンク０～Ｎ－１、すなわち、領域２５３１～２５３Ｎに格納されたログの管理番号領域２５４１から管理番号を読み出せば、管理番号に基づいてそのログが新しいか古いかを判断できる。この判断は、次のようにして行なう。すなわち、連続する２つのバンクｎ，ｎ＋１（ｎはＮの剰余系）が保持する管理番号が不連続である場合、バンクｎには最新のログが、バンクｎ＋１には最も古いログが保持されている。さらに、詳細な説明は、後述する。

【００８５】

以降では、特に断らない限り、管理番号に関する表記および演算は全てＭの剰余系においてログメモリ２５３の領域２５３１～２５３Ｎを指定するバンクの番号に関する表記および演算は全てＮの剰余系における表記および演算を示している。

【００８６】

ライセンスＩＤ領域２５４２は、セッションの対象となるライセンスＬＩＣを特定するライセンスＩＤ（ＬＩＤ）を格納する。Ｋｓ２ｘ領域２５４３は、セッションにおいてライセンスＬＩＣの受信側のデータ記憶装置によって生成されたセッション鍵Ｋｓ２ｘを格納する。

【００８７】

ＳＴ１領域２５４４は、動作中のセッションにおける処理の状態を示すステータスＳＴ１を格納する。ＳＴ２領域２５４５は、ライセンスＩＤ領域２５４２に格納されるライセンスＩＤに対応したライセンスの記憶状態を示すステータスＳＴ２を格納する。

【００８８】

ＫＰｃｍｘ領域２５４６は、ライセンスを移動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデータ記憶装置のクラス公開鍵ＫＰｃｍｘを格納する。ＬＢＡ領域２５４７は、各セッションにおいてライセンスＬＩＣを読出あるいは記憶するために指示されたＬＢＡを格納する。

【００８９】

一連のセッションの処理が進行するにつれて、上記各領域のデータが更新ある

いは参照されていく。ステータスＳＴ１は、”受信待”、”受信済”、”送信待”および”送信済”の４状態のいずれかであり、ステータスＳＴ２は、”データ有”、”データ無”および”移動済”の３状態のいずれかである。

【００９０】

そして、セッション中に予期しない異常が発生し、セッションが中断した場合、そのセッションにおいて送受信されていたライセンスＬＩＣに対して、ログメモリ２５３内のライセンスＩＤ領域２５４１に格納されているライセンスＩＤと、ＬＢＡ領域２５４７に格納されたＬＢＡとによって当該ライセンスＬＩＣの記憶状態が確認され、その確認結果に応じてステータスＳＴ２が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ２５３内に格納されているライセンスＬＩＣ、セッション鍵Ｋｓ２ｘ、ステータスＳＴ１およびステータスＳＴ２を受取って、自身が記録するログの内容と受取ったライセンスＬＩＣ、セッション鍵Ｋｓ２ｘ、ステータスＳＴ１およびステータスＳＴ２とを確認することにより、再度のライセンスの送信を行なってもよいか否かの判断がされる。

【００９１】

なお、セッション鍵Ｋｓ２ｘは、各セッションを特定するために記憶され、セッション鍵Ｋｓ２ｘを共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

【００９２】

また、ステータスＳＴ２には、出力ログが出力される際に、ログメモリ２５３に格納されているライセンスＩＤ（ＬＩＤ）とＬＢＡとによってセキュアデータ記憶部２５０における対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

【００９３】

詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

【００９４】

再び図６を参照して、ＨＤ２０のデータ記録部に関して説明する。ＨＤ２０は

、さらに、暗号化コンテンツデータを記憶するノーマルデータ記憶部２７０を含む。ノーマルデータ記憶部２７０は、データが記憶される円盤状の磁気記録媒体２７０１と、磁気記録媒体２７０１を回転させるモータ２７０２と、モータ２７０２を制御するサーボ制御部２７０３と、磁気記録媒体２７０１上における磁気ヘッドの位置を制御するシーク制御部２７０４と、磁気ヘッドへデータの記録および再生を指示する記録再生処理部２７０５とを含む。

【００９５】

ＨＤ２０は、さらに、ＡＴＡインターフェース部２１２を介して外部との間でデータ授受、制御情報ＡＣに基づくライセンスの出力に関する判断、およびセキュアデータ記憶部２５０の管理などのＨＤ２０内の動作を制御するためのコントローラ２１４を含む。

【００９６】

なお、ノーマルデータ記憶部２７０、ＡＴＡインターフェース部２１２および端子２１０を除く他の構成は、耐タンパモジュール領域に構成される。

【００９７】

図８を参照して、ノーマルデータ記憶部２７０の構成は、一般の公知のハードディスクの構成と変わるところはなく、データ記憶部２７００を含む。データ記憶部２７００は、領域２８００～２８０Ａ（Ａ＝ｍａｘＬＢＡ、ｍａｘＬＢＡは自然数）の各々は、暗号化コンテンツデータおよび暗号化コンテンツデータの付属データ、ライセンステーブル等を格納する。そして、領域２８００～２８０Ａに対応してＬＢＡ：０～ｍａｘＬＢＡが付与されており、各領域２８００～２８０Ａは、ＬＢＡ：０～ｍａｘＬＢＡによって指定され、暗号化コンテンツデータ等のデータは、指定された各領域２８００～２８０Ａに入出力される。

【００９８】

なお、ライセンステーブルは、暗号化コンテンツデータとライセンスの関係を示す情報テーブルであり、ライセンステーブルを参照することで、暗号化コンテンツデータに対応するライセンスと、そのライセンスが記憶されているＬＢＡを特定することができる。したがって、ライセンステーブルは、暗号化コンテンツデータの記憶、削除時、あるいはライセンスの記憶、移動、削除時にその内容が

変更される。

【００９９】

したがって、ＨＤ２０は、ＬＢＡ：０～ｍａｘＬＢＡによって指定できるノーマルデータ記憶部２７０と、それに続くＬＢＡ：ｍａｘＬＢＡ＋１～ｍａｘＬＢＡ＋Ｌによって指定できるセキュアデータ記憶部２５０、より具体的には、ライセンスメモリ２５１に対してデータあるいはライセンスの入出力が行なうことができる。

【０１００】

また、ノーマルデータ記憶領域２７０およびライセンス領域２５１に対するＬＢＡの値については、本実施の形態に限るものではない。

【０１０１】

なお、セキュアデータ記憶部２５０は、通常のアクセスコマンドではＡＴＡインタフェース部２１２を介して、直接、外部からアクセスできない等の手段を設けることで耐タンパ性を確保した、耐タンパ構造を備えている。

【０１０２】

また、ＨＤ２０のセキュアデータ記憶部２５０は、全て半導体メモリによって構成されるものとして説明したが、耐タンパ性を確保した上で、セキュアデータ記憶部２５０の一部あるいはその全てを、磁気記録媒体２７０１上に記憶する構成としてもよい。

【０１０３】

以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１０４】

［配信］

まず、図１に示すデータ配信システムにおいて、ライセンス提供装置４０から端末装置１０に装着されたＨＤ２０へライセンスを配信する動作について説明する。

【０１０５】

図９および図１０は、図１に示すデータ配信システムにおいて、端末装置１０

のユーザが端末装置１０から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンスがライセンス提供装置４０から端末装置１０に装着されたＨＤ２０へ向けて送信され、ＨＤ２０に記憶される際の処理（配信セッション）を説明するための第１および第２のフローチャートである。

【０１０６】

図９における処理開始以前に、端末装置１０のユーザは、端末装置１０をモデム１０６によりネットワーク３０に接続し、端末装置１０をネットワーク３０を介してライセンス提供装置４０に接続していることを前提としている。

【０１０７】

図９を参照して、端末装置１０のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置１０のコントローラ１０８は、バスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へクラス証明書の出力要求を出力する（ステップＳ１）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してクラス証明書の出力要求を受理すると（ステップＳ２）、バスＢＳ３を介して認証データ保持部２０２からクラス証明書Ｃｍ１＝ＫＰｃｍ1／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を読出し、クラス証明書Ｃｍ１をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３）。

【０１０８】

端末装置１０のコントローラ１０８は、ＨＤ２０からＨＤインターフェース部１１０およびバスＢＳ２を介してクラス証明書Ｃｍ１を受理すると（ステップＳ４）、受理したクラス証明書Ｃｍ１をモデム１０６およびネットワーク３０を介してライセンス提供装置４０へ送信する（ステップＳ５）。

【０１０９】

ライセンス提供装置４０では、端末装置１０からクラス証明書Ｃｍ１を受信すると（ステップＳ６）、受信したＣｍ１が正当なクラス証明書であるか否かを認証する（ステップＳ７）。認証処理は次のように行なわれる。

【０１１０】

ライセンス提供装置４０は、クラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を受理すると、ＨＤ２０から出力されたクラス証明書Ｃｍ１に含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を認証部４１８において認証鍵ＫＰａで復号し、ハッシュ値Ｈ（ＫＰｍ１／／Ｉｃｍ１）を抽出する。そして、さらに、認証部４１８は、クラス証明書Ｃｍ１に含まれるＫＰｃｍ１／／Ｉｃｍ１のハッシュ値を演算し、クラス証明書Ｃｍ１から抽出したハッシュ値と演算したハッシュ値とを比較する。配信制御部４１２は、認証部４１８における復号処理結果から、上記の復号ができ、かつ、２つのハッシュ値の値が一致したと判断すると、ＨＤ２０から受理したクラス証明書Ｃｍ１は、正当な証明書であると判断する。

【０１１１】

ステップＳ７において、クラス証明書Ｃｍ１が正当な証明書であると判断された場合、配信制御部４１８は、クラス公開鍵ＫＰｃｍ１を受理する（ステップＳ８）。そして、次の処理（ステップＳ９）へ移行する。正当なクラス証明書でない場合には、クラス証明書Ｃｍ１を受理しないでエラー通知を端末装置１０へ出力し（図１０のステップＳ４４）、端末装置１０においてエラー通知が受理されると（図１０のステップＳ４５）、配信セッションが終了する。

【０１１２】

ステップＳ８においてクラス公開鍵ＫＰｃｍ１が受理されると、配信制御部４１２は、ライセンスＩＤ（ＬＩＤ）を生成し（ステップＳ９）、さらに制御情報ＡＣを生成する（ステップＳ１０）。そして、セッション鍵発生部４１４は、配信のためのセッション鍵Ｋｓ１ａを生成する（ステップＳ１１）。セッション鍵Ｋｓ１ａは、認証部４１８によって得られたＨＤ２０に対応するクラス公開鍵ＫＰｃｍ１によって、暗号処理部４２０によって暗号化され、暗号データＥ（ＫＰｃｍ１，Ｋｓ１ａ）が生成される（ステップＳ１２）。

【０１１３】

そして、配信制御部４１２は、ライセンスＩＤ（ＬＩＤ）および暗号化されたセッション鍵Ｋｓ１ａを１つのデータ列ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）として、バスＢＳ１および通信装置４５０を介して端末装置１０へ向けて出力す

る（ステップＳ１３）。

【０１１４】

端末装置１０は、ネットワーク３０を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受信すると（ステップＳ１４）、受信したＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）をＨＤ２０へ出力する（ステップＳ１５）。そして、ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理する（ステップＳ１６）。コントローラ２１４は、バスＢＳ３を介して受理したＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部２３０へ与え、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２０に固有なクラス秘密鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ａを復号し、セッション鍵Ｋｓ１ａを受理する（ステップＳ１７）。

【０１１５】

ＨＤ２０のコントローラ２１４は、ライセンス提供装置４０で生成されたセッション鍵Ｋｓ１ａの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０においてセッション鍵Ｋｓ１ａが受理された旨の通知を受理すると、ＨＤ２０にセッション鍵の生成の要求通知をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ１８）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部２２６に対してセッション鍵の生成を指示する。そして、セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成する（ステップＳ１９）。

【０１１６】

そして、コントローラ２１４は、セキュアデータ記憶部２５０のログメモリ２５３から最も古いをログが格納されているバンクを検索し、その検索したバンクｎ（０≦ｎ≦Ｎ－１）の管理番号領域２５４１、ライセンスＩＤ領域２５４２、Ｋｓ２ａ領域２５４３、ＳＴ１領域２５４４に対して、それぞれ、新たな管理番

号、ステップＳ１６で受理したライセンスＩＤ、ステップＳ１９において生成されたセッション鍵Ｋｓ２ａ、および”受信待”を格納する（ステップＳ２０）。したがって、バンクｎに格納されるログは最も新しいログとなる。このとき、ログを構成する他の領域については、その内容を初期化、たとえば、全て”０”としてもよいし、そのままの状態であってもよい。

【０１１７】

ここで、図１１を参照して、ステップＳ２０の詳細な動作について説明する。図１１は、ステップＳ２０の詳細な動作を示すフローチャートである。、コントローラ２１４は、ステップＳ１９の後、ログメモリ２５３のうち、最新のログが記録されているログ領域に対応するバンクｎ－１を特定し、そのバンクｎ－１によって指定されるログ領域に格納された履歴情報に含まれる管理番号ｍを取得する（ステップＳ２０ａ）。

【０１１８】

図１２を参照して、ステップＳ２０ａの詳細な動作について説明する。図１２は、ステップＳ２０のさらに詳細なフローチャートである。コントローラ２１４は、ステップＳ１９の後、変数ｎに対して領域２５３２を示すバンク１のバンク番号１を設定し（ステップＳ２０ｃ）、バンク０に格納されている管理番号を取得して、変数ｍに代入する（ステップＳ２０ｄ）。そして、コントローラ２１４は、ログメモリ２５３のバンクｎに格納されている管理番号を取得して、変数ｍａに代入する（ステップＳ２０ｅ）、ｍａ－ｍを演算して演算結果が”１”であるか否かを判定する（ステップＳ２０ｆ）。演算結果が”１”であるとき、コントローラ２１４は、変数ｎに、１を加えたｎ＋１を代入し（ステップＳ２０ｇ）、変数ｍａに代入されている管理番号を変数ｍに代入する（ステップＳ２０ｈ）。その後、ステップＳ２０ｅ～Ｓ２０ｈが繰返し行なわれる。

【０１１９】

ステップＳ２０ｆにおいて、コントローラ２１４は、演算結果が”１”でないとき、バンクｎ－１が、最新のログが記録されている領域であると判断し、最新の管理番号ｍの取得を終了し、図１１に示すステップＳ２０ｂへ移行する。このとき、最も古いログはバンクｎに格納されている。

【０１２０】

ステップＳ２０ｆにおいて、演算結果が”１”であると判定された場合に、ステップＳ２０ｇ，Ｓ２０ｈ，Ｓ２０ｅ，Ｓ２０ｆが、順次、行なわれるのは、演算結果が”１”である場合、変数ｍと変数ｍａとに代入された管理番号ｍと管理番号ｍａとが連続した番号であり、バンクｎ－１とバンクｎとに、前後してログが格納されたことを示している。つまり、ログメモリ２５３の領域はバンク番号順に巡回的に使用され、かつ、管理番号もＭの剰余系において巡回的に使用されるのであるから連続して格納された場合、連続するバンクに格納された管理番号の差は”１”となるからである。したがって、バンクｎ－１には、最新のログが格納されていないことが判る。なお、バンクｎについては不明である。そして、判断する領域を１つ進めて、バンクｎに格納されているログについて判定する。すなわち、バンクｎに格納されているログの管理と、次の領域であるバンクｎ＋１に格納されているログの管理番号に基づいて判定する。フローチャートでは、ステップＳ２０ｇにおいて、ｎにはｎ＋１が代入されることで次の領域に対する判定となる。

【０１２１】

このように、ステップＳ２０ｆ，Ｓ２０ｇ，Ｓ２０ｈ，Ｓ２０ｅのループを繰返し行なうことによってバンク０から順にバンクＮ－１まで連続した領域に格納された管理番号が連続しているか否かが判定される。なお、バンクＮ－１と比較されるのはバンク０の番号である、上述したように、バンクの番号に対する演算はＮの剰余系においてなされる。すなわち、バンクＮ－１の判定においては、ｎ－１＝Ｎ－１、ｎ＝０である。

【０１２２】

ステップＳ２０ｆにおいて、演算結果が”１”でない場合に、バンクｎ－１に格納されたログを最新のログと判定するのは、この場合、バンクｎ－１およびバンクｎに格納される２つのログの管理番号が不連続であるからである。すなわち、上述したように、前後してログの管理番号は連続する。逆に連続しない管理番号を含むログは連続しないこととなる。

【０１２３】

また、図１２に従ってバンクｎ－１を特定するためには、ＨＤ２０の出荷時におけるログメモリ２５３の初期化によってログメモリ２５３の全ての領域２５３１～２５３Ｎに、すなわち、バンク０～バンクＮ－１に対して、所定の管理番号を含むログを格納しておく必要がある。管理番号として全てのバンクに対して同じ値、あるいは、連続するバンクに連続する値（一ヶ所不連続となる）を持つログを格納しておく。なお、ログの他の領域については、いずれの値であってもよい。

【０１２４】

再び、図１１を参照して、上述した方法によって最新の履歴情報（ログ）が記録されているバンクｎ－１と、バンクｎ－１に格納された管理番号ｍとを取得した後、コントローラ２１４は、バンクｎに、管理番号ｍ＋１、ステップＳ１６で受理したライセンスＩＤ、ステップＳ１９で受理したセッション鍵Ｋｓ２ａを格納し、ＳＴ１領域２５４５のステータスＳＴ１を”受信待”に設定する（ステップＳ２０ｂ）。これにより、図９に示すステップＳ２０の動作が終了し、ステップＳ２１へ移行する。

【０１２５】

再び、図９を参照して、ステップＳ２０の後、暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ａによって、切換スイッチ２６２の接点ＰｄとＰｆとを順に切換えることによって与えられるセッション鍵Ｋｓ２ａと個別公開鍵ＫＰｏｍ２とからなる１つのデータ列を暗号化し、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）生成する（ステップＳ２１）。そして、暗号処理部２２４は、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をバスＢＳ３に出力する。バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）は、コントローラ２１４により受理され、コントローラ２１４は、受理した暗号化データとライセンスＩＤ（ＬＩＤ）とを１つのデータ列としたデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２２）。

【０１２６】

そして、端末装置１０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をＨＤ２０から受理すると（ステップＳ２３）、受理したデータをネットワーク３０を介してライセンス提供装置４０に出力する（ステップＳ２４）。

【０１２７】

ライセンス提供装置４０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）を受信すると（ステップＳ２５）、復号処理部４２２においてセッション鍵Ｋｓ１ａによる復号処理を実行し、ＨＤ２０で生成されたセッション鍵Ｋｓ２ａ、およびＨＤ２０の個別公開鍵ＫＰｏｍ２を受理する（ステップＳ２６）。

【０１２８】

配信制御部４１２は、ライセンスＩＤ（ＬＩＤ）に対応するデータＩＤ（ＤＩＤ）およびコンテンツ鍵Ｋｃをコンテンツ格納ＤＢ４０２から取得し（ステップＳ２７）、ライセンスＩＤ（ＬＩＤ）および制御情報ＡＣと併せた１つのデータ列としてのライセンスＬＩＣ＝Ｋｃ／／ＡＣ／／ＤＩＤ／／ＬＩＤを生成する。

【０１２９】

配信制御部４１２は、生成したライセンスＬＩＣを暗号処理部４２４に与える。暗号処理部４２４は、復号処理部４２２によって得られたＨＤ２０の個別公開鍵ＫＰｏｍ２によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を生成する（ステップＳ２８）。そして、暗号処理部４２６は、暗号処理部４２４から受ける暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を、復号処理部４２２から受けるセッション鍵Ｋｓ２ａによって暗号化し、暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を生成する（ステップＳ２９）。

【０１３０】

図１０を参照して、配信制御部４１２は、バスＢＳ１および通信装置４５０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を端末装置１０へ向けて出力する（ステップＳ３０）。端末装置１０は、ネットワーク３０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受理すると（ステップＳ３１）、受理した暗号化データをＨＤ２０へ出力する（ステップＳ３２）。

【０１３１】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受理すると（ステップＳ３３）、バスＢＳ３へ出力する。復号処理部２２８は、セッション鍵発生部２２６から与えられたセッション鍵Ｋｓ２ａを用いてバスＢＳ３に出力されたデータＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を復号し、ＨＤ２０において、ライセンスＬＩＣが個別公開鍵ＫＰｏｍ２により暗号化された暗号化ライセンスＥ（ＫＰｏｍ２，ＬＩＣ）が受理される（ステップＳ３４）。そして、復号処理部２２８は、暗号化ライセンスＥ（ＫＰｏｍ２，ＬＩＣ）をバスＢＳ３へ出力する。

【０１３２】

コントローラ２１４の指示によって、暗号化ライセンスＥ（ＫＰｏｍ２，ＬＩＣ）は、復号処理部２１６において個別秘密鍵Ｋｏｍ２によって復号され、ライセンスＬＩＣが受理される（ステップＳ３５）。

【０１３３】

ＨＤ２０のコントローラ２１４は、ライセンスＬＩＣの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０においてライセンスＬＩＣが受理された旨の通知を受理すると、ＨＤ２０のセキュアデータ記憶部２５０において、その受信したライセンスＬＩＣを格納するＬＢＡ（「格納ＬＢＡ」と呼ぶ。）をバスＢＳ２およびＨＤインターフェース１１０を介してＨＤ２０へ出力する（ステップＳ３６）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してライセンスＬＩＣの格納ＬＢＡを受理すると（ステップＳ３７）、その受理した格納ＬＢＡをログメモリ２５３のバンクｎに格納されたログのＬＢＡ領域２５４７に記憶する（ステップＳ３８）。

【０１３４】

そして、コントローラ２１４は、受理したライセンスＬＩＣに含まれるライセンスＩＤ（ＬＩＤ）と、ステップＳ１６において受理したライセンスＬＩＤ（Ｌ

ＩＤ）とを比較し、一致しているか否かをチェックする（ステップＳ３９）。コントローラ２１４は、ＬＩＤが一致しており、受理したライセンスＬＩＣが正しいものであると判断すると、端末装置１０から受理したセキュアデータ記憶部２５０内のＬＢＡに、受理したライセンスＬＩＣを記憶する（ステップＳ４０）。

【０１３５】

コントローラ２１４は、指定されたＬＢＡにライセンスＬＩＣを記憶すると、有効フラグ領域２５２のそのＬＢＡに対応するフラグを”有効”にする（ステップＳ４１）。そして、コントローラ２１４は、さらに、ログメモリ２５３のバンクｎに格納されたログのＳＴ１領域２５４４のステータスＳＴ１を”受信済”に変更し（ステップＳ４２）、配信セッションにおける一連の処理が終了したことを端末装置１０に通知する。

【０１３６】

そして、端末装置１０において、ＨＤ２０から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

【０１３７】

一方、ステップＳ３９において、コントローラ２１４は、ＬＩＤが一致せず、受理したライセンスＬＩＣが正しくないと判断すると、エラー通知を端末装置１０へ出力し（ステップＳ４３）、端末装置１０は、エラー通知を受理すると（ステップＳ４５）、処理を終了する。

【０１３８】

図９および図１０に示された配信処理においては、ライセンス提供装置４０におけるログの記録に関する記載がなされていないが、図４に示すように、ライセンス提供装置４０には、十分な記憶容量を持つログＤＢ４０４が備えられており、配信セッションにおける各ステップにおけるログがログＤＢ４０４に記憶される。また、ログＤＢ４０４には、ライセンスの送信に伴なう課金情報なども記憶される。

【０１３９】

図９および図１０に示された配信処理における一連の処理において、ステップＳ２５からステップＳ４４の処理中に異常が発生して処理が中断したときは、再

書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置１０の電源が遮断されたり、ライセンス提供装置４０側の異常、あるいは端末装置１０とライセンス提供装置４０との通信異常など、種々の異常ケースが考えられる。ここで、ＨＤ２０内のログメモリ２５３に格納されたステータスＳＴ２を除く出力ログの内容がすべて格納されたステップＳ２２終了後からステップＳ４４までの処理中に処理が中断した場合には、ＨＤ２０は、再書込処理を行なってライセンスの提供を受けることが可能である。ここでは、端末装置１０の判断によって再書込処理を行なうものとしたため、端末装置１０において処理の進行が確認できるステップＳ２２からステップＳ２４を除く、ステップＳ２５からステップＳ４４の処理中に処理が中断した場合を再書込処理の対象とし、他のステップにおける処理の中断においてはライセンス提供装置４０からライセンスの提供がなされなかったものと判断し、図９および図１０に示したフローチャートに従って、最初から処理を行なうこととした。

【０１４０】

同様に、ライセンス提供装置４０がライセンスを出力するまでのライセンス提供装置４０内のステップＳ２５からステップＳ３０までの処理については、端末装置１０において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書込処理の対象から除外して、図９および図１０に示したフローチャートにしたがって、最初から処理を行なうものとしてもよい。

【０１４１】

[配信における再書込]

図１３～図１５は、図９および図１０において示した配信処理におけるステップＳ２５からステップＳ４４の処理中に異常が発生したときに行なわれる再書込処理の第１から第３のフローチャートであり、図１６は、図１３のステップＳ１１２ａの詳細な動作を説明するためのフローチャートである。

【０１４２】

図１３を参照して、端末装置１０は、ステップＳ２５からステップＳ４４の処理中に異常が発生したと判断すると、ライセンスＬＩＣのＬＩＤ／／再書込要求をネットワーク３０を介してライセンス提供装置４０へ出力する（ステップＳ１

０１）。配信制御部４１２は、通信装置４５０およびバスＢＳ１を介してＬＩＤ／／再書込要求を受理すると（ステップＳ１０２）、セッション鍵発生部４１４にセッション鍵を生成するように指示する。指示を受けたセッション鍵発生部４１４は、再書込処理のためのセッションキー鍵Ｋｓ１ｂを生成する（ステップＳ１０３）。そして、配信制御部４１２は、このセッションにおいてＨＤ２０とやり取りしたログが格納されているログＤＢ４０２からＨＤ２０に対応するクラス公開鍵ＫＰｃｍ１を取得し（ステップＳ１０４）、暗号処理部４２０に与える。クラス公開鍵ＫＰｃｍ１を受けた暗号処理部４２０は、クラス公開鍵ＫＰｃｍ１をによりセッション鍵Ｋｓ１ｂを暗号化し、Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）が生成される（ステップＳ１０５）。そして、配信制御部４１２は、ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ１および通信装置４５０を介して端末装置１０へ向けて出力する（ステップＳ１０６）。

【０１４３】

端末装置１０は、ネットワーク３０を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理すると（ステップＳ１０７）、受理したＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）をＨＤ２０へ出力する（ステップＳ１０８）。そして、ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理する（ステップＳ１０９）。コントローラ２１４は、受理したＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ３を介して復号処理部２３０へ与え、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２０に固有なクラス秘密鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ｂを復号し、セッション鍵Ｋｓ１ｂが受理される（ステップＳ１１０）。

【０１４４】

ＨＤ２０のコントローラ２１４は、ライセンス提供装置４０で生成されたセッション鍵Ｋｓ１ｂの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０においてセッション鍵Ｋｓ１ｂが受理された旨の通知を受理すると、ログの

出力要求をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ１１１）。

【０１４５】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してログの出力要求通知を受理し（ステップＳ１１２）、ログの複製処理を行なう（ステップＳ１１２ａ）。

【０１４６】

ここで、図１６を参照して、ステップＳ１１２ａの詳細な動作について説明する。コントローラ２１４は、ログメモリ２５３のうち、最新のログが格納されたバンクｎ－１の特定と、バンクｎ－１に格納されているログの管理番号ｍとを取得する（ステップＳ１１２ｂ）。このステップＳ１１２ｂの詳細な動作は、図１１および図１２に示すフローチャートに従って行なわれる。

【０１４７】

ステップＳ１１２ｂの後、コントローラ２１４は、変数ｋ（ｋは自然数、１≦ｋ≦Ｎ）に”１”を、変数ＥＲＲに”偽”を代入し（ステップＳ１１２ｃ）、バンクｎ－ｋに格納されたログのライセンスＩＤ（ＬＩＤ）が、ステップＳ１０９で受理したライセンスＩＤ（ＬＩＤ）に一致するか否かを判定する。すなわち、コントローラ２１４は、ステップＳ１１２ｂで検出した最新のログに格納されたライセンスＩＤ（ＬＩＤ）が、ステップＳ１０９で受理したライセンスＩＤ（ＬＩＤ）に一致するか否かを判定する。

【０１４８】

２つのライセンスＩＤ（ＬＩＤ）が不一致である場合、コントローラ２１４は、ｋがＮ（バンクの総数）よりも小さいか否かを判定し（ステップＳ１１２ｅ）、ｋがＮ以上であるとき、全てのバンクに対して確認が終了し、つまり、受理したライセンスＩＤ（ＬＩＤ）に一致するＬＩＤを記録したログが格納されていないことが確認され、ステップＳ１１２ｈへ進み、変数ＥＲＲに”真”を代入する（ステップＳ１１２ｈ）。そして、図１３のステップＳ１１３ａに戻り、変数ＥＲＲを確認する。

【０１４９】

再び、図１３を参照して、コントローラ２１４は、変数ＥＲＲを確認する（ステップＳ１１３ａ）。図１６のステップＳ１１２ｈから移行した場合、変数ＥＲＲは”真”であり、該当するライセンスＩＤを記録するログが、ログメモリ２５３に格納されていなかったことを示しているので処理を継続することはできない。したがって、図１５に示すステップＳ１６０へ移行し、エラー通知を端末装置１０へ出力する（ステップＳ１６０）。そして、端末装置１０は、エラー通知を受理し（ステップＳ１６１）、書込拒否により一連の動作が終了する。

【０１５０】

図１６を参照して、ステップＳ１１２ｅにおいて、コントローラ２１４は、ｋはＮよりも小さいと判定すると、全てのバンクに対する確認が終了していないので、今、確認したログより、１つ古いログを確認するために、変数ｋにｋ－１を代入する（ステップＳ１１２ｆ）、ステップＳ１１２ｄへ移行する。そして、コントローラ２１４は、バンクｎ－ｋに格納されたライセンスＩＤ（ＬＩＤ）が、ステップＳ１０９で受理したライセンスＩＤ（ＬＩＤ）と一致するか否かを判定する。この場合、変数ｋの値は”２”であるので、コントローラ２１４は、バンクｎ－２に格納されたログのライセンスＩＤ（ＬＩＤ）が、ステップＳ１０９で受理したライセンスＩＤ（ＬＩＤ）に一致するか否かを判定する。そして、２つのライセンスＩＤ（ＬＩＤ）が不一致である場合、ステップＳ１１２ｅ，Ｓ１１２ｆ，Ｓ１１２ｄが行なわれる。

【０１５１】

このように、コントローラ２１４は、最新のログから、より古いログが格納されるバンクへ向けて、各バンクに格納されたライセンスＩＤ（ＬＩＤ）が、ステップＳ１０９で受理したライセンスＩＤ（ＬＩＤ）と一致するか否かを判定する。そして、この動作（ステップＳ１１２ｅ，Ｓ１１２ｆ，Ｓ１１２ｄ）は、ステップＳ１０９で受理したライセンスＩＤ（ＬＩＤ）に一致するライセンスＩＤ（ＬＩＤ）が検出されるまで、あるいは、全てのバンクの確認が終了するまで繰返し行なわれる。なお、バンク番号はＮの剰余系であるので、ライセンスＩＤの確認は、バンクｎ－１（ｋ＝１），ｎ－２（ｋ＝２），・・・，１（ｋ＝ｎ－１），０（ｋ＝ｎ），Ｎ－１（ｋ＝ｎ＋１），・・・，ｎ（ｋ＝Ｎ）の順に確認され

る。

【０１５２】

ステップＳ１１２ｄにおいて、２つのライセンスＩＤ（ＬＩＤ）が一致したとき、コントローラ２１４は、バンクｎ－ｋに格納されたログを取得し、その取得したログの管理番号ｍをｍ＋１に変更した後、そのログをバンクｎに格納する（ステップＳ１１２ｇ）。つまり、コントローラ２１４は、ライセンス提供装置４０から送信されたライセンスＩＤ（ＬＩＤ）に一致するライセンスＩＤ（ＬＩＤ）を含むログがログメモリ２５３に格納されている場合、そのログ（複数有る場合は、より新しいログ）を、最も古いログが格納されたバンクｎに複製する。この場合、管理番号のみは複製されず、複製したログが新しいログとして扱われるよう先のバンクｎ－１に格納されたログの管理番号に１を加えた値を記録する。したがって、最も古いログは削除され、そこに、現在、進行中の再書込処理に対する新たなログが格納される。

【０１５３】

その後、図１３に示すステップＳ１１３ａへ移行する。

再び、図１３を参照して、コントローラ２１４は、変数ＥＲＲを格納する（ステップＳ１３３ａ）。図１６に示すステップＳ１１２ｇから移行した場合、変数ＥＲＲは”偽”であり、該当するライセンスＩＤを記録したログがバンクｎに複製されるので処理の継続が可能であると判断され、ステップＳ１１３へ移行して、ログメモリ２５３のバンクｎに格納された格納ＬＢＡに記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）と、ログメモリ２５３に格納されたライセンスＩＤ（ＬＩＤ）とが一致するか否かをチェックする（ステップＳ１１３）。

【０１５４】

コントローラ２１４は、両ライセンスＩＤ（ＬＩＤ）が一致すると判断すると、配信処理としては、ライセンス提供装置４０からのライセンスＬＩＣの受理までは行なわれ、ＨＤ２０においてライセンスＬＩＣは受理していると認識する。そうすると、コントローラ２１４は、ログメモリ２５３のバンクｎに格納された格納ＬＢＡにより指定された領域に記憶されるライセンスに対応する有効フラグ領域２５２に格納されているフラグをチェックして、そのライセンスの有効性を

チェックする（ステップＳ１１４）。

【０１５５】

コントローラ２１４は、ライセンスが有効であると判断すると、ログメモリ２５３のバンクｎに格納されたログのステータスＳＴ２を”データ有”に変更し、次の処理（ステップＳ１１８）へ移行する。一方、コントローラ２１４は、ステップＳ１１４においてライセンスが無効であると判断すると、ログメモリ２５３のバンクｎに格納されたログのステータスＳＴ２を”移動済”に変更し、次の処理（ステップＳ１１８）へ移行する。

【０１５６】

ステップ１１３において、コントローラ２１４は、比較したライセンスＩＤ（ＬＩＤ）が一致しないと判断したときは、ログメモリ２５３のバンクｎに格納されたログのステータスＳＴ２を”データ無”に変更する（ステップＳ１１７）。

【０１５７】

ステータスＳＴ２の変更処理がなされると、コントローラ２１４は、ログメモリ２５３のバンクｎからライセンスＩＤ（ＬＩＤ）、ステータスＳＴ１，ＳＴ２およびセッション鍵Ｋｓ２ｃを取得する（ステップＳ１１８）。ここで、この処理は図９および図１０のフローチャートに従って配信セッションの中断に対する処理であるためログメモリ２５３のバンクｎに格納されているセッション鍵はＫｓ２ａであるが、説明の関係上、ログメモリ２５３のバンクｎから取得したセッション鍵をＫｓ２ｃとしている。そして、コントローラ２１４は、取得したセッション鍵Ｋｓ２ｃをバスＢＳ３を介して暗号処理部２２４へ出力する。

【０１５８】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによって、バスＢＳ３から取得したセッション鍵Ｋｓ２ｃを暗号化し、Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）生成する（ステップＳ１１９）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）をバスＢＳ３に出力する。バスＢＳ３に出力されたＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）は、コントローラ２１４により受理され、コントローラ２１４は、ステップＳ１１８において取得したデータとともに１つのデータ列ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ

２ｃ）／／ＳＴ１／／ＳＴ２を生成し、ハッシュ関数を用いてハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を生成する（ステップＳ１２０）。そして、コントローラ２１４は、ハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）をバスＢＳ３を介して暗号処理部２２４へ出力する。

【０１５９】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによって、バスＢＳ３から取得したハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を暗号化し、Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））生成する（ステップＳ１２１）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をバスＢＳ３に出力する。ここで、データ列ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を受信ログと称し、Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））は、受信ログに対してセッション鍵Ｋｓ１ｂを用いて電子署名を行なった署名データである。また、ログメモリ２５３に格納されていたセッション鍵Ｋｓ２ｃをセッション鍵Ｋｓ１ｂを用いて暗号化するのは、セッション鍵Ｋｓ２ｃの漏洩によるライセンスの流出の危険性を排除するためである。

【０１６０】

コントローラ２１４は、バスＢＳ３から署名データを受理すると、ステップＳ１１８において取得した受信ログを用いて、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を生成し、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ１２２）。

【０１６１】

端末装置１０は、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）

／／ＳＴ１／／ＳＴ２））をＨＤ２０から受理すると（ステップＳ１２３）、受理したデータをネットワーク３０を介してライセンス提供装置４０へ出力する（ステップＳ１２４）。そして、ライセンス提供装置４０は、ネットワーク３０を介して署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を受信する。（ステップＳ１２５）

図１４を参照して、ライセンス提供装置４０は、受信した署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））の検証を行なう（ステップＳ１２６）。検証処理は次のように行なわれる。

【０１６２】

配信制御部４１２は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号処理部４２２へ出力するとともに、セッション鍵発生部４１４にセッション鍵Ｋｓ１ｂを発生するように指示する。そして、復号処理部４２２は、セッション鍵Ｋｓ１ｂによって署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号し、ＨＤ２０にて演算したハッシュ値を抽出する。一方、配信制御部４１２は、署名付き受信ログの前半部である受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２のハッシュ値を演算し、復号処理部４２２により復号されたＨＤ２０で演算されたハッシュ値と比較する。配信制御部４１２は、２つのハッシュ値が一致したと判断すると、ＨＤ２０から受理したデータ列は、正当なデータを含むものとしてライセンス提供装置４０において承認される。

【０１６３】

ステップＳ１２６においてＨＤ２０から受理した署名付き受信ログが承認されると、配信制御部４１２は、受理したライセンスＩＤ（ＬＩＤ）に基づいてログＤＢ４０４を検索する（ステップＳ１２７）。配信制御部４１２は、受理したライセンスＩＤ（ＬＩＤ）がログＤＢ４０４内に格納されており、ＨＤ２０に対して確かに提供を行なったライセンスであると判断すると、受理したステータスＳ

Ｔ１，ＳＴ２の内容を確認する（ステップＳ１２８）。

【０１６４】

配信制御部４１２は、ステータスＳＴ１が”受信待”であり、ステータスＳＴ２が”データ無”であるとき、ＨＤ２０に送信したはずのライセンスＬＩＣが何らかの異常によりＨＤ２０において受理されていないと判断し、受信したデータ列に含まれる暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）を復号処理部４２２へ出力してセッション鍵Ｋｓ１ｂによってセッション鍵Ｋｓ２ｃを復号する。そして、復号されたセッション鍵Ｋｓ２ｃは、バスＢＳ１を介して配信制御部４１２へ出力され、配信制御部４１２においてセッション鍵Ｋｓ２ｃが受理される（ステップＳ１２９）。

【０１６５】

そして、配信制御部４１２は、異常発生時のセッション鍵Ｋｓ２ａを今回受理したセッション鍵Ｋｓ２ｃと比較チェックする（ステップＳ１３０）。配信制御部４１２は、セッション鍵Ｋｓ２ａとセッション鍵Ｋｓ２ｃとが一致していると判断すると、ライセンスＬＩＣの再書込に対する許可通知を端末装置１０へ出力する（ステップＳ１３３）。

【０１６６】

一方、ステップＳ１２６においてＨＤ２０から受理したデータ列が承認されなかったとき、ステップＳ１２７においてＨＤ２０から受理したライセンスＩＤ（ＬＩＤ）がログＤＢ４０４内に格納されておらず、ＨＤ２０に対して提供を行なったライセンスであると判断できないとき、ステップＳ１２８において、ＨＤ２０においてライセンスＬＩＣが受理されたものと判断されたとき、またはステップＳ１３０において、セッション鍵Ｋｓ２ａがセッション鍵Ｋｓ２ｃと一致しないと判断されたときは、配信制御部４１２は、ライセンスの再送信は不可と判断し、バスＢＳ１および通信装置４５０を介してエラー通知を端末装置１０へ向けて出力し（ステップＳ１３１）、端末装置１０は、ネットワーク３０を介してエラー通知を受理すると（ステップＳ１３２）、処理が終了する。すなわち、ライセンス提供装置４０において、ライセンスの再書込が拒否されて処理が終了する。

【０１６７】

端末装置１０のコントローラ１０８は、ステップＳ１３３においてライセンス提供装置４０が出力した許可通知を受理すると（ステップＳ１３４）、ＨＤ２０に対するセッション鍵の生成の要求通知をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ１３５）。

【０１６８】

ＨＤ２０は、ライセンス提供装置４０からの再書込処理許可通知に基づいて、端末装置１０からセッション鍵の生成要求通知を受理すると、新たにセッション鍵Ｋｓ２ｂを生成し（ステップＳ１３６）、ログメモリ２５３のバンクｎのログに記録されているセッション鍵Ｋｓ２ｃ（＝Ｋｓ２ａ）を、生成したセッション鍵Ｋｓ２ｂに、ログのステータスＳＴ１を”受信待”に変更する（ステップＳ１３７）。

【０１６９】

以下、ステップＳ１３８からの一連の処理は、図９および図１０において説明したステップＳ２１から処理終了までの一連の処理において、セッションＫｓ２ａに代えて新たに生成してセッション鍵Ｋｓ２ｂが使用される他は、同様の処理が行なわれる。したがって、ステップＳ１３８からの一連の処理の説明は繰返しになるので省略する。

【０１７０】

なお、図１３～図１５のフローチャートに示されるライセンスの配信における再書込処理中の中断に対しては、ステップＳ１０１～Ｓ１３１、ステップＳ１３３およびステップＳ１４２～Ｓ１６０のいずれかのステップにおいて処理が中断した場合には、再び図１３～図１５のフローチャートに従って再書込処理を行なうことができる。一方、ステップＳ１３４～Ｓ１４１のいずれかのステップにおいて処理が中断した場合には、図９および図１０のフローチャートに示されるライセンスの配信処理を最初から行なうことによって、処理を再開することができる。

【０１７１】

このようにして、端末装置１０に装着されたＨＤ２０が正規のクラス証明書Ｃ

ｍ１を保持する機器であることを確認したうえで、クラス証明書Ｃｍ１に含まれて送信されたクラス公開鍵ＫＰｃｍ１によってライセンス提供装置４０およびＨＤ２０でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができる。これによって、不正なハードディスクへのライセンスの配信を禁止することができ、データ配信システムのセキュリティを向上させることができる。

【０１７２】

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置であるＨＤ２０における署名付き受信ログをライセンス提供装置４０へ送信することで、ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことができる。

【０１７３】

［複製・移動］

図１７は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図１７を参照して、端末装置１０にデータ記憶装置として２台のＨＤ２０，２１が装着可能であり、端末装置１０を介してＨＤ２０からＨＤ２１へライセンスの複製または移動が行なわれる。

【０１７４】

ここで、ＨＤ２１は、ＨＤ２０と異なるデータ記憶装置であるため、ＨＤ２０とは異なる個別公開鍵ＫＰｏｍ５と個別秘密鍵Ｋｏｍ５とを保持している。この場合、ＨＤ２１における識別子ｚは、ＨＤ２０のｚ＝２とは異なるｚ＝５となる。また、ＨＤ２１のクラスは、ＨＤ２０のクラスと同じｙ＝１として以下説明する。すなわち、ＨＤ２０、ＨＤ２１とも、クラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，ＫＰｃｍ１／／Ｉｃｍ１）およびクラス秘密鍵Ｋｃｍ１を保持する。しかしながら、ＨＤ２１のクラスがＨＤ２０のクラスと異なる（ｙ≠１）場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、ＨＤ２０とは異なったものとなる。

【０１７５】

図１８および図１９は、図１７に示すライセンスの複製・移動が可能なシステムにおいて、端末装置１０のユーザが端末装置１０から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置１０を介して端末装置１０に装着されたＨＤ２０からＨＤ２１へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための第１および第２のフローチャートである。

【０１７６】

図１８を参照して、端末装置１０のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置１０のコントローラ１０８は、バスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２１へクラス証明書の出力要求を出力する（ステップＳ２０１）。ＨＤ２１においては、端子２１０およびＡＴＡインターフェース部２１２を介してクラス証明書の出力要求が受理されると（ステップＳ２０２）、コントローラ２１４は、認証データ保持部２０２からクラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を読出し、クラス証明書Ｃｍ１をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２０３）。

【０１７７】

端末装置１０は、ＨＤ２１からクラス証明書Ｃｍ１を受理すると（ステップＳ２０４）、受理したクラス証明書Ｃｍ１をＨＤ２０へ送信する（ステップＳ２０５）。

【０１７８】

ＨＤ２０では、端末装置１０からＨＤ２１のクラス証明書Ｃｍ１を受理すると（ステップＳ２０６）、認証部２２０およびコントローラ２１４によって受理したＨＤ２１のクラス証明書Ｃｍ１が正当なクラス証明書であるか否かを認証する（ステップＳ２０７）。認証処理は、ライセンス提供装置４０における認証処理（図９のステップＳ７）と同一であるため詳細な説明は省略する。

【０１７９】

ステップＳ２０７において、コントローラ２１４は、正当なＨＤ２１のクラス証明書でないと判定した場合には、ＨＤ２１のクラス証明書Ｃｍ１を非承認として受理せず、エラー通知を端末装置１０へ出力する（図１９のステップＳ２５２）。そして、端末装置１０においてエラー通知が受理されると（図１５のステップＳ２５３）、配信セッションが終了する。

【０１８０】

ステップＳ２０７において、ＨＤ２１のクラス証明書Ｃｍ１が正当な証明書であると判断されると、ＨＤ２０のコントローラ２１４は、ＨＤ２１のクラス証明書Ｃｍ１を承認し、セッション鍵Ｋｓ１ａを生成するようにセッション鍵発生部２２６を制御し、セッション鍵発生部２２６は、セッション鍵Ｋｓ１ａを生成する（ステップＳ２０９）。

【０１８１】

セッション鍵Ｋｓ１ａは、認証部２２０によって得られたＨＤ２１のクラス公開鍵ＫＰｃｍ１によって、暗号処理部２２２において暗号化され、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）が生成される（ステップＳ２１０）。

【０１８２】

そして、コントローラ２１４は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）を、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２１１）。

【０１８３】

端末装置１０は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）を受理すると（ステップＳ２１２）、受理した暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）をＨＤ２１へ出力する（ステップＳ２１３）。ここで、ライセンスＩＤ（ＬＩＤ）は、事前に管理ファイルを参照することで端末装置１０が取得している。管理ファイルは、ＨＤ２０に記憶されている暗号化コンテンツデータとライセンスとの関係を管理するための管理データを記録したデータファイルであって、ノーマルデータ記憶部２７０に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

【０１８４】

そして、ＨＤ２１においては、コントローラ２１４が、端子２１０およびＡＴＡインターフェース部２１２を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理する（ステップＳ２１４）。続いて、コントローラ２１４は、バスＢＳ３を介してＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部２３０へ与え、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２１に固有なクラス秘密鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ａを復号し、セッション鍵Ｋｓ１ａを受理する（ステップＳ２１５）。

【０１８５】

ＨＤ２１のコントローラ２１４は、ＨＤ２０で生成されたセッション鍵Ｋｓ１ａの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０は、ＨＤ２１においてセッション鍵Ｋｓ１ａが受理された旨の通知を受理すると、セッション鍵の生成の要求通知をＨＤ２１へ出力する（ステップＳ２１６）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部２２６に対してセッション鍵の生成を指示する。そして、セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成する（ステップＳ２１７）。

【０１８６】

セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成すると、バスＢＳ３を介してコントローラ２１４へ出力し、コントローラ２１４は、セッション鍵Ｋｓ２ａを受ける。そして、コントローラ２１４は、最も古いログを格納したバンクを検索し、そこに処理中のセッションに対するログを新たに格納する（ステップＳ２１８）。ステップＳ２１８の詳細な動作は、図１１および図１２に示すフローチャートに従って行なわれる。ただし、ＨＤ２１における処理と、ＨＤ２０における同様の処理結果を区別するために最も古いログを格納したバンクは、バンクｎａであるとする。すなわち、図１１および図１２に示すフローチャートにおける変数ｎを変数ｎａと読替えればよい。

【０１８７】

したがって、ログメモリ２５３のバンクｎａに、バンクｎａ－１に格納される

ログの管理番号に１を加えた新しい管理番号と、ステップＳ２１４において受理したライセンスＩＤ（ＬＩＤ）とセッション鍵Ｋｓ２ａとを格納し、ステータスＳＴ１を”受信待”にする。

【０１８８】

続いて、ＨＤ２１においては、続いて、暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ａによって、切換スイッチ２６２の接点ＰｄとＰｆとを順に切換えることによって与えられるセッション鍵Ｋｓ２ａと個別公開鍵ＫＰｏｍ５とからなる１つのデータ列を暗号化し、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）を生成する（ステップＳ２１９）。そして、暗号処理部２２４は、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）をバスＢＳ３に出力する。バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）は、コントローラ２１４により受理され、コントローラ２１４は、受理した暗号化データとライセンスＩＤ（ＬＩＤ）とを１つのデータ列としたデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２２０）。

【０１８９】

そして、端末装置１０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）をＨＤ２１から受理すると（ステップＳ２２１）、受理したデータをＨＤ２０へ出力する（ステップＳ２２２）。

【０１９０】

ＨＤ２０では、端子２１０およびＡＴＡインタフェース部１１０を介してデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）を受理すると（ステップＳ２２３）、復号処理部２２８においてセッション鍵Ｋｓ１ａによる復号処理を実行し、ＨＤ２１で生成されたセッション鍵Ｋｓ２ａ、およびＨＤ２１の個別公開鍵ＫＰｏｍ５を抽出して受理する（ステップＳ２２４）。そして、復号処理部２２８は、復号したセッション鍵Ｋｓ２ａをバスＢＳ３を介してコントローラ２１４へ出力し、コントローラ２１４は、セッション鍵Ｋｓ２ａを受ける。そして、コントローラ２１４は、最も古いログを格納したバンクに、処理中のセッショ

ンに対するログを新たに格納する（ステップＳ２２５）。ステップＳ２２５の詳細な動作は、図２０に示すフローチャートに従って行なわれる。図２０を参照して、ステップＳ２２５は、ログメモリ２５３の最新ログが記録されたバンクｎ－１を特定し、かつ、バンクｎ－１に格納された管理番号ｍを取得するステップＳ２２５ａと、バンクｎに、管理番号ｍ＋１、ライセンスＩＤ（ＬＩＤ）、セッション鍵Ｋｓ２ａ、およびクラス公開鍵ＫＰｃｍｙを格納し、かつ、ステータス領域を“送信待”に設定するステップＳ２２５ｂとから成る。そして、ステップＳ２２５ａの詳細な動作は、図１２に示すフローチャートに従って行なわれる。したがって、コントローラ２１４は、図２０および図１２に示すフローチャートに従って、ステップＳ２２３において受理したライセンスＩＤ（ＬＩＤ）とステップＳ２２４で受理したセッション鍵Ｋｓ２ａとをバンクｎに格納し、ステータスＳＴ１を“送信待”にする。

【０１９１】

ＨＤ２０では、ステップＳ２２５の処理を終えると、ＨＤ２０のコントローラ２１４は、その旨をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０からの通知を受理すると、ＨＤ２０のセキュアデータ記憶部２５０において、ＨＤ２０からＨＤ２１へ送信するライセンスＬＩＣが格納されているＬＢＡ（格納ＬＢＡ）をバスＢＳ２およびＨＤインターフェース１１０を介してＨＤ２０へ出力する（ステップＳ２２６）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して送信対象のライセンスＬＩＣの格納ＬＢＡを受理すると（ステップＳ２２７）、その受理した格納ＬＢＡをセキュアデータ記憶部２５０のログメモリ２５３のバンクｎに記憶する（ステップＳ２２８）。

【０１９２】

そして、コントローラ２１４は、受理した格納ＬＢＡに格納されるライセンスＬＩＣに対応する有効フラグ領域２５２のフラグが“有効”であるか“無効”であるかを確認する（ステップＳ２２９）。コントローラ２１４は、有効フラグが“有効”であると、格納ＬＢＡに格納されているライセンスＬＩＣを取得する（

ステップＳ２３０）。

【０１９３】

図１９を参照して、ＨＤ２０では、コントローラ２１４が、対象のライセンスＬＩＣを取得すると、ライセンスＬＩＣに含まれるライセンスＩＤ（ＬＩＤ）と、ステップＳ２２３において受理し、ログメモリ２５３のバンクｎａに格納されているログに記憶されているライセンスＩＤ（ＬＩＤ）とを比較し、一致しているか否かをチェックする（ステップＳ２３１）。コントローラ２１４は、一致していると判断すると、取得したライセンスＬＩＣに含まれる制御情報ＡＣを確認して利用制限がかけられていないかをチェックする（ステップＳ２３２）。

【０１９４】

コントローラ２１４は、制御情報ＡＣにおいてライセンスＬＩＣの利用が禁止されていないことを確認すると、取得したライセンスＬＩＣを暗号処理部２３２に与える。暗号処理部２３２は、復号処理部２２８によって得られたＨＤ２１の個別公開鍵ＫＰｏｍ５によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を生成する（ステップＳ２３３）。そして、暗号処理部２３２は、暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を切替スイッチＰｃを介して暗号処理部２２４へ出力し、暗号処理部２２４は、暗号処理部２３２から受けた暗号化データを復号処理部２２８から受けたセッション鍵Ｋｓ２ａによって暗号化し、暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を生成する（ステップＳ２３４）。

【０１９５】

続いて、コントローラ２１４は、対象のライセンスＬＩＣに含まれる制御情報ＡＣに基づいて、ＨＤ２０からＨＤ２１へのライセンスＬＩＣの送信が「移動」であるか「複製」であるかを確認する（ステップＳ２３５）。コントローラ２１４は、「移動」であると確認したときは、その対象のライセンスＬＩＣに対応する、すなわち、格納ＬＢＡに対応する有効フラグ領域２５２のフラグを“無効”に変更する（ステップＳ２３６）。一方、コントローラ２１４は、「複製」であると確認したときには、当該ライセンスＬＩＣがＨＤ２０に残っていてもよいので、有効フラグ領域２５２のフラグの変更は行なわずに次の処理（ステップＳ２

３７）へ移行する。

【０１９６】

コントローラ２１４は、有効フラグ領域２５２の処理が終わると、ログメモリ２５３のバンクｎに格納されているログのステータスＳＴ１を“送信済”に変更し（ステップＳ２３７）、ＡＴＡインターフェース部２１２および端子２１０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を端末装置１０へ送信する（ステップＳ２３８）。

【０１９７】

一方、ステップＳ２２９において受理した格納ＬＢＡに対応する有効フラグ領域２５２のフラグが“無効”であったとき、ステップＳ２３１においてライセンスＩＤ（ＬＩＤ）が一致しないとき、または、ステップＳ２３２において、取得したライセンスＬＩＣに含まれる制御情報ＡＣにより当該ライセンスＬＩＣの利用が禁止されているときは、コントローラ２１４は、端末装置１０に対してエラー通知を出力し（ステップＳ２５２）、端末装置１０においてエラー通知が受理されると（ステップＳ２５３）、処理が終了する。

【０１９８】

端末装置１０は、ステップＳ２３８においてＨＤ２０から出力された暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受理すると（ステップＳ２３９）、受理した暗号化データをＨＤ２１へ出力する（ステップＳ２４０）。

【０１９９】

ＨＤ２１では、コントローラ２１４が、端子２１０およびＡＴＡインターフェース部２１２を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受理し（ステップＳ２４１）、バスＢＳ３へ出力する。復号処理部２２８は、セッション鍵発生部２２６から与えられたセッション鍵Ｋｓ２ａを用いてバスＢＳ３に出力されたデータＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を復号し、ＨＤ２１において、ライセンスＬＩＣが個別公開鍵ＫＰｏｍ５により暗号化された暗号化ライセンスＥ（ＫＰｏｍ５，ＬＩＣ）が受理される（ステップＳ２４２）。そして、復号処理部２２８は、暗号化ライセンスＥ（ＫＰｏｍ５，ＬＩＣ）をバスＢＳ３へ出力する。

【０２００】

コントローラ２１４の指示によって、暗号化ライセンスＥ（ＫＰｏｍ５，ＬＩＣ）は、復号処理部２１６において個別秘密鍵Ｋｏｍ５によって復号され、ＨＤ２１においてライセンスＬＩＣが受理される（ステップＳ２４３）。

【０２０１】

コントローラ２１４は、ライセンスＬＩＣの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２１においてライセンスＬＩＣが受理された旨の通知を受理すると、ＨＤ２１のセキュアデータ記憶部２５０において、その受信したライセンスＬＩＣを格納するＬＢＡ（格納ＬＢＡ）をバスＢＳ２およびＨＤインターフェース１１０を介してＨＤ２１へ出力する（ステップＳ２４４）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してライセンスＬＩＣを格納する格納ＬＢＡを受理すると（ステップＳ２４５）、その受理した格納ＬＢＡをログメモリ２５３のバンクｎに格納されるログのＬＢＡ領域２５４４に記録する（ステップＳ２４６）。

【０２０２】

そして、コントローラ２１４は、受理したライセンスＬＩＣに含まれるライセンスＩＤ（ＬＩＤ）と、ステップＳ２１４において受理したライセンスＬＩＤ（ＬＩＤ）とを比較し、一致しているか否かをチェックする（ステップＳ２４７）。コントローラ２１４は、ＬＩＤが一致しており、受理したライセンスＬＩＣが正しいものであると判断すると、端末装置１０から受理したセキュアデータ記憶部２５０内の格納ＬＢＡに対応する領域に、受理したライセンスＬＩＣを記憶する（ステップＳ２４８）。

【０２０３】

コントローラ２１４は、指定された格納ＬＢＡにライセンスＬＩＣを記憶すると、有効フラグ領域２５２のその格納ＬＢＡに対応するフラグを“有効”にする（ステップＳ２４９）。そして、コントローラ２１４は、さらに、ログメモリ２５３のバンクｎに格納されたログのステータスＳＴ１を“受信済”にし（ステッ

プＳ２５０）、複製・移動セッションにおける一連の処理が終了したことをＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０に通知する。

【０２０４】

そして、端末装置１０において、ＨＤ２１からの処理終了通知が受理されると、ＨＤ２０からＨＤ２１へのライセンスＬＩＣの複製・移動セッションが正常終了する。

【０２０５】

一方、ステップＳ２４７において、ＨＤ２０のコントローラ２１４が、ＬＩＤが一致しておらず、受理したライセンスＬＩＣが正しくないと判断すると、ＡＴＡインターフェース部２１２および端子２１０を介してエラー通知を端末装置１０へ出力し（ステップＳ２５１）、端末装置１０においてエラー通知が受理されると（ステップＳ２５３）、ＨＤ２０からＨＤ２１へのライセンスＬＩＣの複製・移動セッションが異常終了する。

【０２０６】

ここで、配信セッションのときと同様に、図１８および図１９に示された複製・移動セッションにおける一連の処理において、ステップＳ２２７からステップＳ２５２の処理中に異常が発生し、処理が中断したときは、再書込処理の対象となる。

【０２０７】

ここで、図１８および図１９に示された複製・移動セッションにおいて、ステップＳ２２７からステップＳ２３５までの処理を再書込処理の対象としたのは、この一連の処理がＨＤ２０の内部処理であり、ステップＳ２２６の終了後は、ステップＳ２３８まで端末装置１０においていずれのステップを処理中に処理が中断したかを特定できないため、すべてステップＳ２３６が実行されてライセンスが無効化されたものとし、必ず再書込処理の対象としたものである。

【０２０８】

そして、ステップＳ２３６からステップＳ２４７までの処理を再書込処理の対象としたのは、「移動」の場合、この間は、ＨＤ２０内のライセンスがステップ

Ｓ２３６において無効化され、かつ、ＨＤ２１内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。

【０２０９】

また、ステップＳ２４８からステップＳ２５０までの処理を再書込処理の対象としたのは、ステップＳ２４９，Ｓ２５０については、これらの処理はステップＳ２４８におけるライセンス書込後の処理であるから本来は処理が終了しているところ、端末装置１０からはステップＳ２４８の終了が特定できないため、ステップＳ２４８が終了していないものとみなして、ステップＳ２４８からステップＳ２５０を再書込処理の対象としたものである。なお、ステップＳ２４８が終了していて再書込処理が行なわれた場合には、再書込は拒否される。

【０２１０】

また、ステップＳ２５１の処理を再書込処理の対象としたのは、本来、この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置１０においては、ステップＳ２５１において処理が中断したことを特定することができないため、再書込処理の対象としたものである。

【０２１１】

なお、端末装置１０において、上述したように当該セッションがライセンスの「複製」であると判断できる場合、あるいはステップＳ２２７からステップＳ２３５およびステップＳ２４９からステップＳ２５１のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書込処理とする必要はなく、図１８および図１９に示された複製・移動セッションを再度実行すればよい。

【０２１２】

［移動／複製における再書込］

図２１～図２３は、図１８および図１９において示した複製・移動セッションの処理フローにおけるステップＳ２２７からステップＳ２５２の処理中に異常が発生したときに行なわれる再書込処理の第１から第３のフローチャートである。

【０２１３】

図２１を参照して、端末装置１０は、ステップＳ２２７からステップＳ２５２の処理中に異常が発生したと判断すると、ライセンスＩＤ（ＬＩＤ）とライセンスＬＩＣの再送要求とをデータ列ＬＩＤ／／再送要求としてＨＤ２０へ出力する（ステップＳ３０１）。ＨＤ２０では、コントローラ２１４が、端子２１０およびＡＴＡインターフェース部２１２を介してＬＩＤ／／再送要求を受理する（ステップＳ３０１ａ）。そして、ログの複製処理を行なう（３０１ｂ）。複製処理では、ログメモリ２５３内にステップＳ３０１ａにおいて受理したＬＩＤを含むログが格納されていないかを検索し、格納されていた場合、ログメモリ２５３の最も古いログを格納しているバンクｎに、検索されたＬＩＤを含むログを複製し、変数ＥＲＲ＝“偽”とする。一方、ログメモリ２５３内にステップＳ３０１ａにおいて受理したＬＩＤを含むログが格納されていない場合には、変数ＥＲＲ＝“真”とする。この複製処理の詳細な動作は、図１６に示すフローチャートに従って行なわれる。

【０２１４】

そして、コントローラ２１４は、ステップＳ３０１ａの処理結果の判定、すなわち、変数ＥＲＲが“真”、“偽”のいずれであるかを判定する（ステップＳ３０１ｂ）。“真”の場合、受理したＬＩＤを含むログがバンクｎへ複製されたことを示すので、再送要求に対する処理を開始するために次のステップＳ３０２へ移行する。“偽”の場合、受理したＬＩＤを含むログがログメモリ２５３に格納されていなかった、つまり、ＨＤ２０において受理したＬＩＤによって特定されるライセンスＬＩＣの入出力処理がなされていなかったことを示すので、再送要求に対応不能と判断し、図２３のステップＳ３７２へ移行し、エラー通知を端末装置１０に対して出力する。端末装置１０においてはエラー通知が受理されると（ステップＳ３７３）、処理が終了する。

【０２１５】

ＨＤ２０において、ステップＳ３０１ｂにおいて変数ＥＲＲ＝”偽”を確認すると、コントローラ２１４は、ログメモリ２５３のバンクｎに複製され、かつ、格納されているログのステータスＳＴ１の状態を確認する（ステップＳ３０２）。コントローラ２１４は、ステータスＳＴ１が“送信待”または“送信済”でな

いとき、すなわち複製・移動セッションにおいてライセンスＬＩＣの送信側でないときは、図２３に示すステップＳ３７１へ処理が移行する。

【０２１６】

ＨＤ２０のコントローラ２１４は、ステータスＳＴ１が“送信待”または“送信済”であるときは、セッション鍵発生部２２６にセッション鍵を生成するように指示し、セッション鍵発生部２２６は、セッション鍵Ｋｓ１ａを生成する（ステップＳ３０３）。セッション鍵Ｋｓ１ｂが生成されると、コントローラ２１４は、中断以前に受理した、ライセンスＬＩＣの移動／複製先のＨＤ２１のクラス公開鍵ＫＰｃｍ１を、ログメモリ２５３のバンクｎに格納されたログから取得する（ステップＳ３０４）。ここで、移動／複製先のＨＤ２１から再びクラス証明書Ｉｍｃ１を受理することなくログに記憶されるクラス公開鍵ＫＰｃｍ１を用いるのは、再書込処理におけるなりすまし攻撃によるライセンスＬＩＣの漏洩を防ぐためである。したがって、再び、クラス証明書Ｉｍｃ１を受理する場合には、ＨＤ２０において、中断した処理において受理したクラス証明書と再書込処理において受理したクラス証明書とが同一か否かを確認する必要がある。たとえば、再書込処理において受理したクラス証明書Ｉｍｃ１に含まれるクラス公開鍵とログに記録されるクラス公開鍵を比較して再書込処理を行なうか否かを判断する。

【０２１７】

そして、ＨＤ２１では、そのクラス公開鍵ＫＰｃｍ１によって、セッション鍵Ｋｓ１ｂが暗号処理部２２２によって暗号化され、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）が生成される（ステップＳ３０５）。コントローラ２１４は、生成された暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）とライセンスＩＤ（ＬＩＤ）とをデータ列ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）としてＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３０６）。

【０２１８】

端末装置１０は、ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理すると（ステップＳ３０７）、受理したＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）をＨＤ２１へ出力する（ステップＳ３０８）。

【０２１９】

ＨＤ２１において、コントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理すると（ステップＳ３０９）、バスＢＳ３を介してＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を復号処理部２３０へ与える。そうすると、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２１に固有なクラス秘密鍵Ｋｃｍ１によって復号処理を実行してセッション鍵Ｋｓ１ｂを復号し、セッション鍵Ｋｓ１ｂを受理する（ステップＳ３１０）。

【０２２０】

ＨＤ２１のコントローラ２１４は、ＨＤ２０で生成されたセッション鍵Ｋｓ１ｂの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介してＨＤ２１からの通知を受理すると、ＨＤ２１のログメモリ２５３に格納されるログのＨＤ２０への出力要求をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２１へ出力する（ステップＳ３１１）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してログの出力要求通知を受理する（ステップＳ３１２）。そして、ＨＤ２０におけるステップＳ３０１ａと同様にログの複製処理を行なう（ステップＳ２１３ａ）。複製処理時、ログメモリ２５３内にステップＳ３０９において受理したＬＩＤを含むログが格納されていないかを検索し、格納されていた場合、ログメモリ２５３の最も古いログを格納しているバンクｎａに、検索されたＬＩＤを含むログを複製し、変数ＥＲＲａ＝“偽”とする。一方、ログメモリ２５３内にステップＳ３０９において受理したＬＩＤを含むログが格納されていない場合には、ＥＲＲａ＝“真”とする。このステップＳ３１２ａの詳細な動作は、図１６に示すフローチャートに従って行なわれる。ただし、ＨＤ２１における処理と、ＨＤ２０における同様の処理結果を区別するために変数ｎを変数ｎａとし、変数ＥＲＲを変数ＥＲＲａとする。すなわち、図１６のステップＳ１１２ｂに相当する図１２に示すフローチャートにおける変数ｎを変数ｎａに、変数ＥＲＲを変数ＥＲＲａにそれぞれ読替えればよい。

【０２２１】

そして、コントローラ２１４は、ステップＳ３１２ａの処理結果の判定、すなわち、ＥＲＲａが“真”、“偽”のいずれであるかを判定する（ステップＳ３２１２ｂ）。“偽”の場合、受理したＬＩＤを含むログがバンクｎａへ複製されたことを示すので、再送要求に対する処理を開始するために次のステップＳ３１３へ移行する。“真”の場合、受理したＬＩＤを含むログがログメモリ２５３に格納されていなかった、つまり、ＨＤ２１において、ステップＳ３１３において受理したＬＩＤによって特定されるライセンスＬＩＣの入出力処理がなされなかったことを示すので、再送要求に対応不能と判断し、図２３のステップＳ３７１へ移行し、エラー通知を端末装置１０に対して出力する。端末装置１０においては、エラー通知が受理されると（ステップＳ３７３）、処理が終了する。

【０２２２】

ＨＤ２１において、ステップＳ３１２ｂにおいてＥＲＲａ＝”偽”を確認すると、コントローラ２１４は、ログメモリ２５３のバンクｎａに格納されているログの格納ＬＢＡに対する領域に記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）と、ログメモリ２５３のバンクｎａに格納されているログのライセンスＩＤ（ＬＩＤ）とが一致するか否かを確認する（ステップＳ３１３）。

【０２２３】

コントローラ２１４は、ライセンスＩＤ（ＬＩＤ）が一致すると、さらに、ログメモリ２５３のバンクｎａに格納されているログの格納ＬＢＡに対応する有効フラグ領域２５２のフラグを確認し、そのライセンスＬＩＣが有効であるか無効であるかを確認する（ステップＳ３１４）。コントローラ２１４は、有効フラグ領域２５２のフラグが“有効”であるときは、ログメモリ２５３のバンクｎａに格納されているログのステータスＳＴ２を“データ有”に変更し（ステップＳ３１５）、次の処理（ステップＳ３１８）へ移行する。一方、コントローラ２１４は、有効フラグ領域２５２のフラグが“無効”であるときは、ログメモリ２５３のバンクｎａに格納されているログのステータスＳＴ２を“移動済”に変更し（ステップＳ３１６）、次の処理（ステップＳ３１８）へ移行する。

【０２２４】

また、コントローラ２１４は、ステップＳ３１３において両ライセンスＩＤ（ＬＩＤ）が一致しないときは、ログメモリ２５３のバンクｎａに格納されているログのステータスＳＴ２を“データ無”に変更する（ステップＳ３１７）。

【０２２５】

ステータスＳＴ２の変更処理がなされると、コントローラ２１４は、ログメモリ２５３のバンクｎａからライセンスＩＤ（ＬＩＤ）、ステータスＳＴ１，ＳＴ２、セッション鍵Ｋｓ２ｃおよび格納ＬＢＡを取得する（ステップＳ３１８）。ここで、この処理は、図９および図１０のフローチャートに従った配信セッションの中断に対する処理であるため、ＨＤ２１のログメモリ２５３に格納されている当該処理のログに記憶されているセッション鍵はＫｓ２ａであるが、説明の関係上、ログメモリ２５３のバンクｎから取得したセッション鍵をＫｓ２ｃとしている。そして、コントローラ２１４は、取得したセッション鍵Ｋｓ２ｃをバスＢＳ３を介して暗号処理部２２４へ出力する。

【０２２６】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによってセッション鍵Ｋｓ２ｃを暗号化し、Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）生成する（ステップＳ３１９）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）をバスＢＳ３に出力する。バスＢＳ３に出力されたＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）は、コントローラ２１４により受理され、コントローラ２１４は、ステップＳ３１８において取得したデータとともに１つの受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を生成し、そのハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を生成する（ステップＳ３２０）。そして、コントローラ２１４は、ハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）をバスＢＳ３を介して暗号処理部２２４へ出力する。

【０２２７】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによって、バスＢＳ３から取得したハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を暗号

化し、署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））生成する（ステップＳ３２１）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をバスＢＳ３に出力する。

【０２２８】

コントローラ２１４は、バスＢＳ３から署名データを取得すると、ステップＳ３１８において取得した受信ログを用いて、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を生成し、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））と格納ＬＢＡとを、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３２２）。

【０２２９】

図２２を参照して、端末装置１０は、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））と格納ＬＢＡとをＨＤ２１から受理すると（ステップＳ３２３）、受理したデータをＨＤ２０へ出力する（ステップＳ３２４）。

【０２３０】

ＨＤ２０において、コントローラ２１４は、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を受理すると（ステップＳ３２５）、受理した署名付き受信ログの検証を行なう（ステップＳ３２６）。検証処理は、以下のように行われる。

【０２３１】

ＨＤ２０のコントローラ２１４は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号処理部２２８へ出

力するとともに、セッション鍵発生部２２６にセッション鍵Ｋｓ１ｂを発生するように指示する。そして、復号処理部２２８は、セッション鍵Ｋｓ１ｂによって署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号し、ＨＤ２１によって求められたハッシュ値を抽出する。一方、ＨＤ２０のコントローラ２１４は、署名付き受信ログの前半部である受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２のハッシュ値を演算し、復号処理部２２８により抽出されたハッシュ値と比較する。ＨＤ２０のコントローラ２１４は、２つのハッシュ値が一致したと判断すると、ＨＤ２１から受理した受信ログは、正当なデータを含むものとしてＨＤ２０において承認される。

【０２３２】

ステップＳ３２６において承認されると、ＨＤ２０のコントローラ２１４は、ステップＳ３２５において承認した受信ログに含まれるライセンスＩＤ（ＬＩＤ）をログメモリ２５３のバンクｎに格納されるライセンスＩＤ（ＬＩＤ）と比較する（ステップＳ３２７）。

【０２３３】

コントローラ２１４は、ライセンスＩＤ（ＬＩＤ）が一致すると、受信ログに含まれる暗号データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）を復号処理部２２８へ出力し、復号処理部２２８は、セッション鍵発生部２２６から受けるセッション鍵Ｋｓ１ｂによってセッション鍵Ｋｓ２ｃを復号し、セッション鍵Ｋｓ２ｃが受理される（ステップＳ３２８）。そして、復号されたセッション鍵Ｋｓ２ｃは、バスＢＳ３を介してコントローラ２１４へ出力される。続いて、コントローラ２１４は、エラー発生時のセッション鍵、すなわち、バンクｎのログに記録されているセッション鍵Ｋｓ２ａと、今回、承認した受信ログに含まれていたセッション鍵Ｋｓ２ｃとを比較する（ステップＳ３２９）。コントローラ２１４は、セッション鍵Ｋｓ２ａとセッション鍵Ｋｓ２ｃとが一致していると判断すると、受理したステータスＳＴ１，ＳＴ２の内容を確認する（ステップＳ３３０）。

【０２３４】

ＨＤ２０のコントローラ２１４は、受信した受信ログのステータスＳＴ１が“

受信待”であり、受信ログのステータスＳＴ２が“データ無”であるとき、ＨＤ２１に送信したはずのライセンスＬＩＣが何らかの異常によりＨＤ２１において受理されていないと判断する。そうすると、ＨＤ２０のコントローラ２１４は、さらに、ログメモリ２５３のバンクｎのログの格納ＬＢＡに記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）と、ログメモリ２５３のバンクｎのログのライセンスＩＤ（ＬＩＤ）とが一致するか否かを確認する（ステップＳ３３１）。ＨＤ２０のコントローラ２１４は、ライセンスＩＤ（ＬＩＤ）が一致すると、さらに、ログメモリ２５３のバンクｎのログの格納ＬＢＡに対応する有効フラグ領域２５２のフラグを確認し、そのライセンスＬＩＣが有効であるか無効であるかを確認する（ステップＳ３３２）。そして、コントローラ２１４は、有効フラグ領域２５２のフラグが“無効”であるときは、その有効フラグ領域２５２のフラグを“有効”に変更する（ステップＳ３３３）。一方、コントローラ２１４は、有効フラグ領域２５２のフラグが“有効”であるときは、次の処理（ステップＳ３３４）へ移行する。そして、コントローラ２１４は、ログメモリ２５３のバンクｎのログの格納ＬＢＡと許可通知とをＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３３４）。

【０２３５】

端末装置１０のコントローラ１０８は、ＨＤ２０からＨＤインターフェース部１１０およびバスＢＳ２を介して対象のライセンスＬＩＣが格納される格納ＬＢＡと許可通知とを受理すると（ステップＳ３３５）、ＨＤ２１に対してセッション鍵の生成の要求通知をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２１へ出力する（ステップＳ３３６）。

【０２３６】

ＨＤ２１は、端末装置１０からセッション鍵の生成要求通知を受理すると、新たにセッション鍵Ｋｓ２ｂを生成し（ステップＳ３３７）、ログメモリ２５３のバンクｎａのログに記憶されているセッション鍵Ｋｓ２ｃ（Ｋｓ２ａ）を、生成したセッション鍵Ｋｓ２ｂに、ログのステータスＳＴ１を“受信待”に変更する（ステップＳ３３８）。

【０２３７】

以下、ステップＳ３３９からの一連の処理は、図１８および図１９において説明したステップＳ２１９から処理終了までの一連の処理において、セッション鍵Ｋｓ２ａに代えて新たに生成したセッション鍵Ｋｓ２ｂが使用される他は、同様の処理が行なわれる。したがって、ステップＳ３３９に続く一連の処理の説明は繰返しになるので省略する。

【０２３８】

なお、ステップＳ３３５において処理を終了し、ＨＤ２０にライセンスを残すことも可能である。この場合、図１８および図１９に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

【０２３９】

なお、図２１～図２３のフローチャートに示されるライセンスの移動または複製における再書込処理の中断に対しては、ステップＳ３０１～Ｓ３４４およびステップＳ３４７～Ｓ３７１のいずれかのステップにおいて処理が中断した場合には、再び図２１～図２３に示されるフローチャートに従って再書込処理を行なうことができる。一方、ステップＳ３２５～Ｓ３４６のいずれかのステップにおいて処理が中断した場合には、図１８および図１９のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

【０２４０】

このようにして、端末装置１０に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先のＨＤ２１から受取ったクラス証明書Ｃｍ１が有効であることを確認し、クラス証明書Ｃｍ１に含まれて送信されたクラス公開鍵ＫＰｃｍ１によってライセンスの複製・移動が行なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンスの複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる

。

【０２４１】

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置であるＨＤ２１における複製・移動セッションの対象となったライセンスＬＩＣに対する受信ログを送信側のデータ記憶装置であるＨＤ２０へ送信し、ＨＤ２０において、自身のログメモリ２５３に格納されるログの内容と、そのログに記憶される格納ＬＢＡによって特定されるセキュアデータ記憶部２５０の領域に記憶されるライセンスＬＩＣとを比較し、さらに有効フラグ領域２５２に記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、２つのデータ記憶装置ＨＤ２０およびＨＤ２１に利用可能なライセンスが重複して存在することのない安全な再書込処理が提供される。

【０２４２】

このように、本発明は、複製・移動セッションの中断によるライセンスＬＩＣの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処理手順を提供するとともに、再書込処理に至った場合でも安全に処理が行なわれ、確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

【０２４３】

なお、図１８～図２３におけるＨＤ２１の処理ステップＳ２０２，２０３，Ｓ２１４，Ｓ２１５，Ｓ２１７～Ｓ２２０，Ｓ２４１～Ｓ２４３，Ｓ２４５～Ｓ２５１，Ｓ３０９，Ｓ３１０，Ｓ３１２～Ｓ３２２，Ｓ３３７～Ｓ３４０，Ｓ３６１～Ｓ３６３，Ｓ３６５～Ｓ３７１は、図９、図１０および図１３～図１５におけるＨＤ２０の処理ステップＳ２，Ｓ３，Ｓ１６，Ｓ１７，Ｓ１９～Ｓ２２，Ｓ３３～Ｓ３５，Ｓ３７～Ｓ４３，Ｓ１０９，Ｓ１１０，Ｓ１１２～Ｓ１２２，Ｓ１３６～Ｓ１３９，Ｓ１５０～Ｓ１５２，Ｓ１５４～Ｓ１６０とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるＨＤ２１の処理とライセンスの配信処理時におけるＨＤ２０の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（ＨＤ２０，ＨＤ２１）においてライセンスを

書込むためのデータ記憶装置における処理である。

【０２４４】

［再生許諾］

再び図５を参照して、コンテンツデータを再生する再生回路１５０を備えた端末装置１０にデータ記憶装置としてのＨＤ２０が装着され、コンテンツデータの再生許諾は、ＨＤ２０から端末装置１０内の再生回路１５０に対して行なわれる。

【０２４５】

図２４は、端末装置１０のユーザが端末装置１０から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置１０に装着されたＨＤ２０から端末装置１０内の再生回路１５０へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

【０２４６】

図２４を参照して、端末装置１０のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置１０のコントローラ１０８は、バスＢＳ２を介して再生回路１５０へクラス証明書の出力要求を出力する（ステップＳ４０１）。再生回路１５０において、認証データ保持部１５０２は、バスＢＳ２からクラス証明書の出力要求を受けると（ステップＳ４０２）、保持しているクラス証明書Ｃｐ３＝ＫＰｃｐ３／／Ｉｃｐ３／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐ３／／Ｉｃｐ３））をバスＢＳ２へ出力する（ステップＳ４０３）。

【０２４７】

コントローラ１０８は、バスＢＳ２からクラス証明書Ｃｐ３を受理すると（ステップＳ４０４）、受理したクラス証明書Ｃｐ３をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ４０５）。

【０２４８】

ＨＤ２０では、端末装置１０からクラス証明書Ｃｐ３を受理すると（ステップＳ４０６）、受理したクラス証明書Ｃｐ３が正当なクラス証明書であるか否かを検証する（ステップＳ４０７）。検証処理は、複製・移動セッションにおけるステップＳ２０７において説明したのと同様の方法で行なわれ、説明は省略する。

【０２４９】

ステップＳ４０７において、クラス証明書Ｃｐ３が正当な証明書であると判断された場合、コントローラ２１４は、クラス証明書Ｃｐ３を承認し、クラス証明書Ｃｐ３に含まれるクラス公開鍵ＫＰｃｐ３を受理する（ステップＳ４０８）。そして、次の処理（ステップＳ４０９）へ移行する。コントローラ２１４は、正当なクラス証明書でない場合には、クラス証明書Ｃｐ３を非承認とし、クラス証明書Ｃｐ３を受理せずにエラー通知を端末装置１０へ出力し（ステップＳ４３５）、端末装置１０においてエラー通知が受理されると（ステップＳ４３６）、再生許諾セッションが終了する。

【０２５０】

ステップＳ４０８においてクラス公開鍵ＫＰｃｐ３が受理されると、ＨＤ２０のセッション鍵発生部２２６は、セッション鍵Ｋｓ１ｄを生成する（ステップＳ４０９）。セッション鍵Ｋｓ１ｄは、受理されたクラス公開鍵ＫＰｃｐ３によって、暗号処理部２２２において暗号化され、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）が生成される（ステップＳ４１０）。

【０２５１】

そして、コントローラ２１４は、暗号処理部２２２からバスＢＳ３を介して暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受けると、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ４１１）。

【０２５２】

端末装置１０において、ＨＤインターフェース部１１０およびバスＢＳ２を介してコントローラ１０８が暗号データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受理すると（ステップＳ４１２）、コントローラ１０８は、受理した暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をバスＢＳ２を介して再生回路１５０へ出力する（ステップＳ４１３）。再生回路１５０の復号処理部１５０６は、バスＢＳ２から暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受理すると（ステップＳ４１４）、Ｋｃｐ保持部１５０４に保持される再生回路１５０に固有なクラス秘密鍵Ｋｃｐ３によって復号処理することによりセッション鍵Ｋｓ１ｄを復号し、セッション鍵Ｋｓ１

ｄが受理される（ステップＳ４１５）。

【０２５３】

セッション鍵Ｋｓ１ｄが受理されると、セッション鍵発生部１５０８は、セッション鍵Ｋｓ２ｄを生成し（ステップＳ４１６）、生成したセッション鍵Ｋｓ２ｄを暗号処理部１５１０に与える。暗号処理部１５１０は、復号処理部１５０６から受けるセッション鍵Ｋｓ１ｄをセッション鍵Ｋｓ２ｄにより暗号化し、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を生成する（ステップＳ４１７）。そして、暗号処理部１５１０は、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）をバスＢＳ２へ出力する（ステップＳ４１８）。

【０２５４】

コントローラ１０８は、バスＢＳ２から暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受理し（ステップＳ４１９）、受理したデータをバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ４２０）。

【０２５５】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受理すると（ステップＳ４２１）、受理したデータをバスＢＳ３へ出力する。復号処理部２２８は、セッション鍵発生部２２６から与えられたセッション鍵Ｋｓ１ｄを用いてバスＢＳ３に出力された暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を復号し、ＨＤ２０においてセッション鍵Ｋｓ２ｄが受理される（ステップＳ４２２）。そして、コントローラ２１４は、セッション鍵Ｋｓ２ｄが受理されると、その旨の通知をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する。

【０２５６】

端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介してＨＤ２０においてセッション鍵Ｋｓ２ｄが受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンスＬＩＣが格納されているセキュアデータ記憶部２５０のＬＢＡをバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する。

【０２５７】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して対象のライセンスＬＩＣが格納されているＬＢＡを受理すると（ステップＳ４２４）、そのＬＢＡに格納されるライセンスＬＩＣに対応する有効フラグ領域２５２のフラグが“有効”であるか“無効”であるかを確認する（ステップＳ４２５）。

【０２５８】

コントローラ２１４は、有効フラグ領域２５２のフラグが“有効”であると、受理したＬＢＡに基づいて、対象のライセンスＬＩＣをセキュアデータ記憶部２５０から取得する（ステップＳ４２６）。そして、コントローラ２１４は、取得したライセンスＬＩＣに含まれる制御情報ＡＣの内容を確認する（ステップＳ４２７）。コントローラ２１４は、制御情報ＡＣにおいて利用回数が指定されているときは、制御情報ＡＣの利用回数を１増分し、次の処理（ステップＳ４２９）へ移行する。一方、コントローラ２１４は、制御情報ＡＣにより再生制限がかけられていないときは、取得したライセンスＬＩＣに含まれるコンテンツ鍵ＫｃをバスＢＳ３へ出力する。

【０２５９】

暗号処理部２２４は、復号処理部２２８から受けるセッション鍵Ｋｓ２ｄによりバスＢＳ３上に出力されたコンテンツ鍵Ｋｃを暗号化して暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を生成し（ステップＳ４２９）、生成したデータをバスＢＳ３へ出力する。そして、コントローラ２１４は、バスＢＳ３上に出力された暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ４３０）。

【０２６０】

端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を受理すると（ステップＳ４３１）、受理したデータをバスＢＳ２へ出力する（ステップＳ４３２）。

【０２６１】

再生回路１５０の復号処理部１５１２は、バスＢＳ２から暗号化データＥ（Ｋ

ｓ２ｄ，Ｋｃ）を受理すると（ステップＳ４３３）、セッション鍵発生部１５０８から与えられるセッション鍵Ｋｓ２ｄを用いて暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を復号する。これにより、再生回路１５０においてコンテンツ鍵Ｋｃが受理され（ステップＳ４３４）、一連の再生許諾セッションの処理が正常終了する。

【０２６２】

一方、ステップＳ４２５において、有効フラグ領域２５２のフラグが“無効”であったとき、またはステップＳ４２７において、制御情報ＡＣに含まれる内容が再生不可であったときは、コントローラ２１４は、端末装置１０に対してエラー通知を出力し（ステップＳ４３５）、端末装置１０においてエラー通知が受理されると（ステップＳ４３６）、再生許諾セッションが終了する。

【０２６３】

このようにして、データ記憶装置であるＨＤ２０から端末装置１０に備えられる再生回路１５０への再生許諾に関しても、再生回路１５０が正規のクラス証明書Ｃｐ３を保持していること、およびクラス証明書Ｃｐ３に含まれて送信されたクラス公開鍵ＫＰｃｐ３が有効であることを確認した上でコンテンツ鍵Ｋｃが再生回路１５０へ送信され、不正なコンテンツデータの再生を禁止することができる。

【０２６４】

なお、フローチャートにおいて図示しないが、再生回路１５０は、コンテンツの再生許諾がなされ、コンテンツ鍵Ｋｃを受理すると、ＨＤ２０から出力された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号処理部１５１４において復号し、再生部１５１６において復号処理部により復号されたデータＤｃが再生され、ＤＡ変換部１５１８によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子１５２０へ再生信号が出力される。

【０２６５】

このように、ＨＤ２０では、ライセンスの漏洩が無いように安全に保護し、記憶、入出力の管理を行なうために、

（１）他の装置（ライセンス提供装置または他のＨＤ）からライセンスの提供を

受けて格納する書込処理（図９および図１０におけるＨＤ２０および図２１～図２３におけるＨＤ２１の処理）

（２）書込処理の中断から、書込処理を再開する再書込処理（図１３～図１５におけるおけるＨＤおよび図２１～図２３におけるＨＤ２１の処理）

（３）他のＨＤに対してライセンスを移動または複製する提供処理（図１６～図１８におけるＨＤ２０の処理）

（４）提供処理の中断から、移動複製処理を再開する再提供処理（ライセンスの提供元としての再書込処理、図２１～図２３におけるＨＤ２０の処理）

（５）暗号化コンテンツデータを復号することを目的として再生回路に対してコンテンツ鍵Ｋｃを提供する再生許諾処理（図２４におけるＨＤ２０の処理）

の５つの処理を、暗号技術によって実現している。

【０２６６】

なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、データの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

【０２６７】

［実施の形態２］

実施の形態１においては、ＨＤ２０は、図１３～図１５のフローチャートに示される再書込処理および図２１～図２３のフローチャートに示される再提供処理において、再書込／提供処理を開始するにあたって、処理の可否を判断するために、再書込／提供処理の対象となるライセンスに対する直前のログを検索する。そして、対応したログが検索された場合、検索したログをログメモリ２５３のバンクｎに複製して、以後の処理においてはバンクｎに格納されたログを処理の手

順に従って更新していくものとして説明した。

【０２６８】

しかし、再書込処理においては、複製したログはライセンスの提供側に対して直前の処理に対するログとして出力した後、図１４のステップＳ１３７において、その内容が書換えられてしまう。ログの複製は、古いログが格納されたバンクから順に新たなログの格納バンクに向けて循環的に使用していくログメモリ２５３の特性に由来するものであり、再書込処理の初期における中断（図１４のステップＳ１３６以前）においても、再書込処理に対応するログが、より長くログメモリ２５３に保持されることを目的としている。

【０２６９】

したがって、十分に大きなログメモリ２５３を備えたＨＤにおいては、再書込処理における検索されたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接出力するように構成することも可能である。この場合、ステータスＳＴ２の変更（ステップＳ１１５，Ｓ１１６，Ｓ１１７）は、当該バンクのログに対して行なわれ、出力するためのログの取得（ステップＳ１１８）は、当該バンクから行なわれることとなる。

【０２７０】

また、ログの複写がなされないため、再書込処理に対応するログを格納するためのバンクは、図１４のステップＳ１３７において確保される。したがって、ステップＳ１３７は、「ログメモリの最も古いログを格納しているバンクｎａに新たなログを格納」と変更される。

【０２７１】

さらに、ＨＤ２１も同様に処理を変更することが可能である。その他の全ての処理は、実施の形態１と同じである。なお、この処理の変更によってライセンスの安全性は何ら変化することはなく、実施の形態１と同様の効果を得ることができる。

【０２７２】

［実施の形態３］

ライセンスの再書込処理と同様に、ライセンスの再提供処理において、検索さ

れたログの複製を行なうことなく、検索されたログが格納されていたバンクから直接読出し、再提供の可否を判定することも可能である。図２１のステップＳ３０１ａにおいて複製を行なうことなく、図２１のステップＳ３０２および図２２のステップＳ３２９，Ｓ３３１，Ｓ３３２において検索されたログが格納されていたバンクから直接ログを取得するように処理を変更すればよい。その他の全ての処理は、実施の形態１と同じである。

【０２７３】

この処理の変更によってライセンスの安全性は、何ら変化することはなく、実施の形態１と同様の効果を得ることができる。また、実施の形態２と組合わせることも可能である。

【０２７４】

［実施の形態４］

ＨＤ２０の実装における処理を軽減するためには、通常の書込処理および再書込処理は、より共通していることが望ましい。そこで、実施の形態１における「セッション鍵要求」移行のＨＤ２０における処理、すなわち、通常の書込処理（図９のステップＳ１９～Ｓ２２、図１０のステップＳ３３～Ｓ３５，Ｓ３８～Ｓ４３）と再書込処理（図１４のステップＳ１３６～Ｓ１３９、図１５のステップＳ１５０～Ｓ１５２，Ｓ１５４～Ｓ１６０）を共通とする。この場合、図９のステップＳ２０と図１４のステップＳ１３７とを同一処理とすることで容易に実現できる。

【０２７５】

この場合、ステップＳ１３７をステップＳ２０と同一処理とし、“ログメモリの最も古いログを格納しているバンクｎｂに新たなログを格納”とする。また、詳細な処理は、図１１および図１２のフローチャートに従い、変数ｎを変数ｎｂと読替えればよい。また、変数ｎを変数ｎｂと読替えるのは、図１３および図１４のステップＳ１３７までの処理における変数ｎと区別するためである。これに伴って、図１４および図１５のステップＳ１３７以降のステップＳ１５４，Ｓ１５５，Ｓ１５９におけるバンクｎを全てバンクｎｂと読替える。

【０２７６】

同様に、移動複製セッションでは、図２１～図２３のフローチャートに示されるステップＳ３４２以降の処理と、図１６～図１８のフローチャートに示されるステップＳ２２２以降の処理との違いが、ログの記録の違い（図２３のステップＳ３４５と図１８のステップＳ２２５との違い）のみである。図２３のステップＳ３４５の処理を図１８のステップＳ２２５と同一の処理とすることによってＨＤ２０の実装を容易にすることができる。この場合、ステップＳ３４５をステップＳ２０と同一処理とし、“ログメモリの最も古いログを格納しているバンクｎｂに新たなログを格納”とする。また、詳細な処理は、図２０および図１２のフローチャートに従い、変数ｎを変数ｎｂと読替えればよい。また、変数ｎを変数ｎｂと読替えるのは、図２１および図２２のステップＳ２４５までの処理における変数ｎと区別するためである。これに伴って、図２３のステップＳ３４５以降のステップＳ３４８，Ｓ５７におけるバンクｎを全てバンクｎｂと読替える。

【０２７７】

その他の全ての処理は、実施の形態１と同一である。また、処理の変更によってライセンスの安全性は何ら変化することなく、実施の形態１と同様な効果を得ることができる。さらに、ＨＤ２１も同様に処理を変更することが可能である。

【０２７８】

このように、通常書込処理および再書込処理の共通化によって、実施の形態１と同様なライセンスの安全な管理を実現した上で実装する処理量の軽減を図ることができる。

【０２７９】

［実施の形態５］

ログの記録開始タイミングを明確にするために、全ての処理においてＨＤ外部からライセンスＩＤ（ＬＩＤ）を受理することによって、ログメモリ２５３からバンクを１つ確保し、当該処理に対するログを記録するように変更した実施の形態５について説明する。

【０２８０】

まず、実施の形態５におけるライセンスの配信動作について説明する。

実施の形態５においては、ライセンス提供措置４０からＨＤ２０へのライセン

スの配信は、図２５および図２６に示すフローチャートに従って行なわれる。図２５および図２６に示すフローチャートは、図９および図１０に示すフローチャートのステップＳ１６とステップＳ１７との間にステップＳ１６ａを挿入し、ステップＳ２０をステップＳ２０１ａに代えたものであり、その他は図９および図１０に示すフローチャートと同じである。

【０２８１】

ステップＳ１６ａの詳細な動作は、図２７に示すフローチャートに従って行なわれる。図２７を参照して、ＨＤ２０にコントローラ２１４は、ステップＳ１６の後、最新のログが格納されているバンクｎ－１を特定し、バンクｎに格納されている管理番号ｍを取得する（ステップＳ１６ｂ）。そして、このステップＳ１６ｂの詳細な動作は、図１２に示すフローチャートに従って行なわれる。

【０２８２】

コントローラ２１４は、ステップＳ１６ｂの後、管理番号ｍ＋１、およびステップＳ１６で受理したライセンスＩＤ（ＬＩＤ）をバンクｎに格納し、バンクｎに格納されたログのＳＴ１領域２５４４を“受信待”に設定する（ステップＳ１６ｃ）。これにより、図２５に示すステップＳ１６ａの動作が終了する。

【０２８３】

また、コントローラ２１４は、ステップＳ１９の後、ログメモリ２５３のバンクｎに格納されたログのＫｓ２ｘ領域２５４３に、ステップＳ１９で受理したセッション鍵Ｋｓ２ａを記録する（ステップＳ２０１ａ）。

【０２８４】

その他は、実施の形態１において説明したとおりである。

[配信における再書込]

実施の形態５におけるライセンスの配信が途中で中断した場合のライセンスの再書込の動作は、図１３～図１５に示すフローチャートに従って行なわれる。その詳細な動作は実施の形態１において説明したとおりである。

【０２８５】

[移動／複製]

図２８および図２９は、図１７に示すライセンスの複製・移動が可能なシステ

ムにおいて、端末装置１０のユーザが端末装置１０から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置１０を介して端末装置１０に装着されたＨＤ２０からＨＤ２１へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための実施の形態５における第１および第２のフローチャートである。

【０２８６】

図２８および図２９に示すフローチャートは、図１８および図１９に示すフローチャートのステップＳ２０７とステップＳ２０９との間にステップＳ２０８を挿入し、ステップＳ２１４とステップＳ２１５との間にステップＳ２１４ａを挿入し、ステップＳ２１８をステップＳ２１８ａに代え、ステップＳ２２５をステップＳ２２５ａに代えたものであり、その他は図１８および図１９に示すフローチャートと同じである。

【０２８７】

図２８を参照して、ＨＤ２０のコントローラ２１４は、ステップＳ２０７においてＨＤ２１からの証明書Ｃｍ１を承認したとき、ログメモリ２５３のうち最も古いログが格納されたバンクｎに新たなログを格納する（ステップＳ２０８）。このステップＳ２０８の詳細な動作は、図３０に示すフローチャートに従って行なわれる。

【０２８８】

図３０を参照して、ステップＳ２０８は、ＨＤ２０においてログメモリ２５３の最新ログが記録されたバンクｎ－１を特定し、かつ、バンクｎ－１に格納された管理番号ｍを取得するステップＳ２０８ａと、バンクｎに、管理番号ｍ＋１、ライセンスＩＤ（ＬＩＤ）、およびクラス公開鍵ＫＰｃｍｙを格納し、かつ、ＳＴ１領域２５４４のステータスＳＴ１を“送信待”に設定するステップＳ２０８ｂとから成る。そして、ステップＳ２０８ａの詳細な動作は、図１２に示すフローチャートに従って行なわれる。したがって、コントローラ２１４は、図１２および図３０に示すフローチャートに従って、ステップＳ２０６において受理したライセンスＩＤ（ＬＩＤ）とＨＤ２１のクラス公開鍵ＫＰｃｍ１と、“送信待”に設定されたステータスＳＴ１とを記録した新たなログをバンクｎに格納する。

【０２８９】

また、ＨＤ２１のコントローラ２１４は、ステップＳ２１４の後、最も古いログが格納されたバンクｎａに新たなログを格納する（ステップＳ２１４ａ）。このステップＳ２１４ａの詳細な動作は、上述した図１２および図２７に示すフローチャートに従って行なわれる。ただし、変数ｎは、変数ｎａに読替える。

【０２９０】

したがって、ＨＤ２１のコントローラ２１４は、図１２および図２７に示すフローチャートに従って、ステップＳ２１４において受理したライセンスＩＤ（ＬＩＤ）と、“受信待”に設定されたステータスＳＴ１とを記録した新たなログを、ログメモリ２５４の中で最も古いログが格納されていたバンクｎａに格納する（ステップＳ２１４ａ）。

【０２９１】

さらに、ＨＤ２１のコントローラ２１４は、ステップＳ２１７の後、ログメモリ２５３のバンクｎａにステップＳ２１７において生成されたセッション鍵Ｋｓ２ａを格納する（ステップＳ２１８ａ）。

【０２９２】

さらに、ＨＤ２０のコントローラ２１４は、ステップＳ２２４の後、ログメモリ２５３のバンクｎに、ステップＳ２２４で受理したセッション鍵Ｋｓ２ａを格納する（ステップＳ２２５ａ）。

【０２９３】

その他は、実施の形態１において説明したとおりである。

[移動／複製における再書込]

実施の形態５におけるＨＤ２１からＨＤ２０へのライセンスの移動・複製セッションが途中で中断した場合のライセンスの再書込動作は、図２１～図２３に示すフローチャートに従って行なわれる。したがって、その詳細な動作は実施の形態１で説明したとおりである。

【０２９４】

このように、実施の形態５では、実施の形態１と同様に安全なライセンスの再書込／提供処理を実現し、かつ、それぞれの処理におけるログの発生タイミング

を明確にするとともに、実施の形態３と同様に、通常書込／再書込処理の共通化によって実装する処理量の軽減を図ることができる。なお、ＨＤ２１も同様に処理を変更することが可能である。

【０２９５】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおいて使用される暗号通信に用いられる鍵、情報等の特性を示す図である。

【図４】　図１に示すライセンス提供装置の構成を示す概略ブロック図である。

【図５】　図１に示す端末装置の構成を示す概略ブロック図である。

【図６】　図１に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

【図７】　図６に示すハードディスクにおけるセキュアデータ記憶部の構成を示す図である。

【図８】　図６に示すハードディスクにおけるノーマルデータ記憶部の構成を示す図である。

【図９】　図１に示すデータ配信システムにおける配信処理を説明するための実施の形態１における第１のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける配信処理を説明するための実施の形態１における第２のフローチャートである。

【図１１】　図９に示すステップＳ２０の詳細な動作を説明するためのフローチャートである。

【図１２】　図１１に示すステップＳ２０ａの詳細な動作を説明するためのフローチャートである。

【図１３】　図１に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態１における第１のフローチャートである。

【図１４】　図１に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態１における第２のフローチャートである。

【図１５】　図１に示すデータ配信システムにおける配信処理中の再書込処理を説明するための実施の形態１における第３のフローチャートである。

【図１６】　図１３に示すステップＳ１１２ａの詳細な動作を説明するためのフローチャートである。

【図１７】　複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

【図１８】　図１７に示すシステムにおける複製または移動処理を説明するための実施の形態１における第１のフローチャートである。

【図１９】　図１７に示すシステムにおける複製または移動処理を説明するための実施の形態１における第２のフローチャートである。

【図２０】　図１８に示すステップＳ２１８の詳細な動作を説明するためのフローチャートである。

【図２１】　図１７に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態１における第１のフローチャートである。

【図２２】　図１７に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態１における第２のフローチャートである。

【図２３】　図１７に示すシステムにおける複製または移動処理中の再書込処理を説明するための実施の形態１における第３のフローチャートである。

【図２４】　図５に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

【図２５】　図１に示すデータ配信システムにおける配信処理を説明するための実施の形態５における第１のフローチャートである。

【図２６】　図１に示すデータ配信システムにおける配信処理を説明するた

めの実施の形態５における第２のフローチャートである。

【図２７】　図２５に示すステップＳ１６ａの詳細な動作を説明するためのフローチャートである。

【図２８】　図１７に示すシステムにおける複製または移動処理を説明するための実施の形態５における第１のフローチャートである。

【図２９】　図１７に示すシステムにおける複製または移動処理を説明するための実施の形態５における第２のフローチャートである。

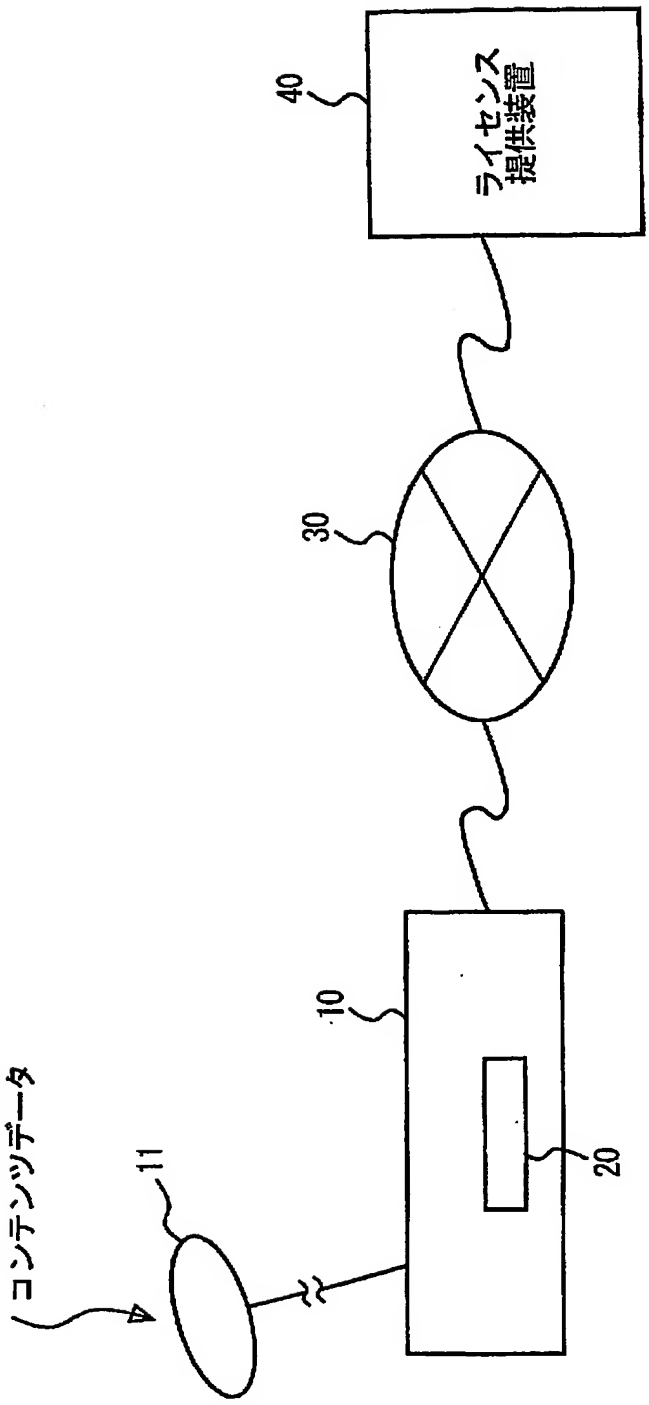
【図３０】　図２８に示すステップＳ２０８の詳細な動作を説明するためのフローチャートである。

【符号の説明】

１０　端末装置、１１　アンテナ、２０，２１　ハードディスクドライブ（ＨＤ）、３０　ネットワーク、４０　ライセンス提供装置、１０２　アンテナ、１０４　受信部、１０６　モデム、１０８　コントローラ、１１０　ＨＤインターフェース部、１５０　再生回路、２０２，１５０２　認証データ保持部、２０４　Ｋｃｍ保持部、２０６　Ｋｏｍ保持部、２０８　ＫＰｏｍ保持部、２１０，１５２０　端子、２１２　ＡＴＡインターフェース部、２１４　コントローラ、２１６，２２８，２３０，４２２，１５０６，１５１２，１５１４　復号処理部、２１８，４１６　ＫＰａ保持部、２２０，４１８　認証部、２２２，２２４，２３２，４２０，４２４，４２６，１５１０　暗号処理部、２２６，４１４，１５０８　セッション鍵発生部、２５０　セキュアデータ記憶部、２５１　ライセンス領域、２５２　有効フラグ領域、２５３　ログメモリ、２６０，２６２　切替スイッチ、２７０　ノーマルデータ記憶部、４０２　コンテンツＤＢ、４０４　ログＤＢ、４１０　データ処理部、４１２　配信制御部、４５０　通信装置、１５０４　Ｋｃｐ保持部、１５１６　再生部、１５１８　ＤＡ変換部、２５４１　管理番号領域　２５４２　ライセンスＩＤ領域、２５４３　Ｋｓ２ｘ領域、２５４４　ＳＴ１領域，２５４５　ＳＴ２領域、２５４６　ＫＰｃｍｘ領域、２５４７　ＬＢＡ領域、２７０１　磁気記録媒体、２７０２　モータ、２７０３　サーボ制御部、２７０４　シーク制御部、２７０５　記録再生処理部、ＢＳ１～ＢＳ３　バス。

【書類名】　図面

【図１】



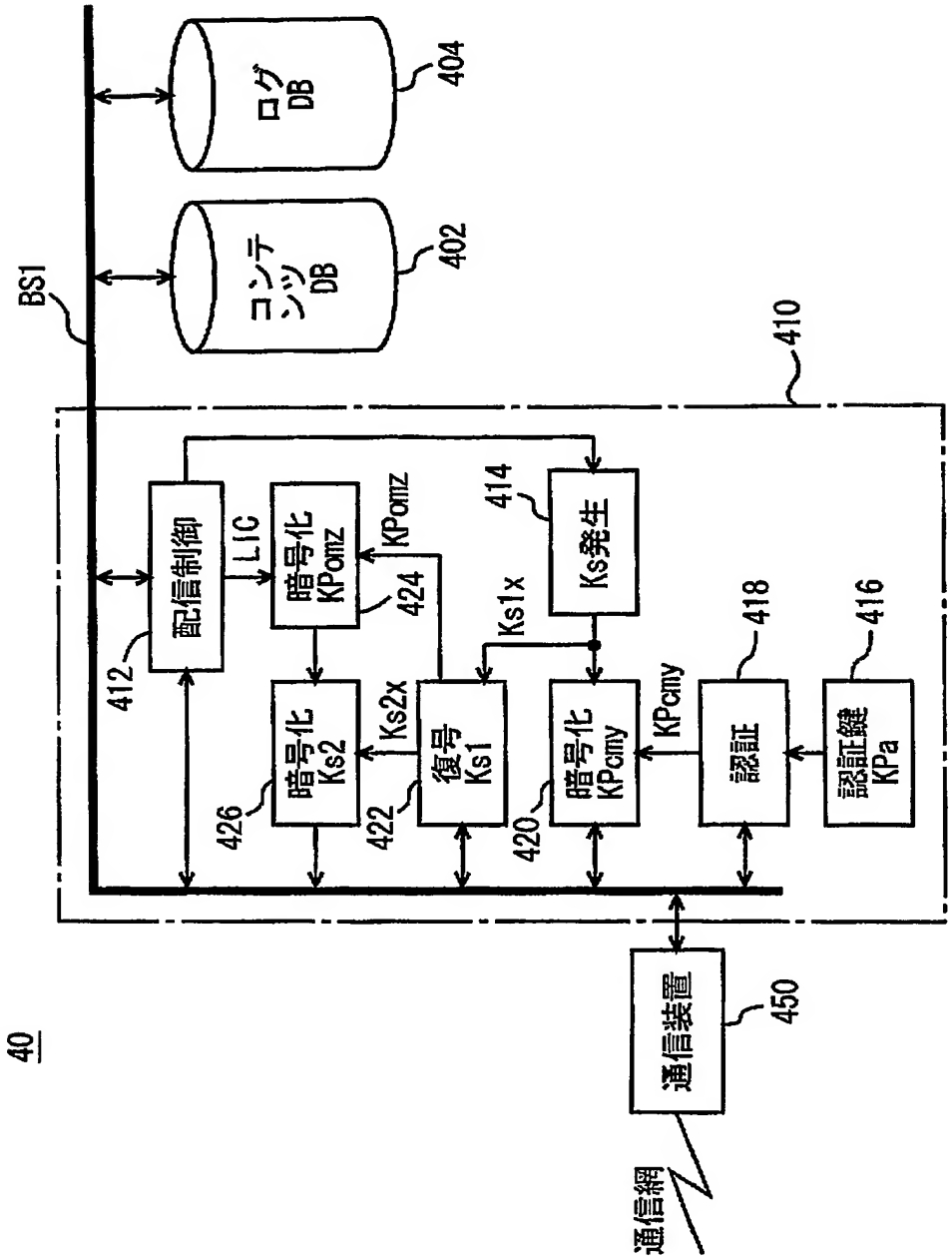
【図２】

記号	名称	属性	特性
Dc	データ	データ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて暗号化した暗号化コンテンツデータ E(Kc, Dc)として記録管理される
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	Dcおよび Kcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

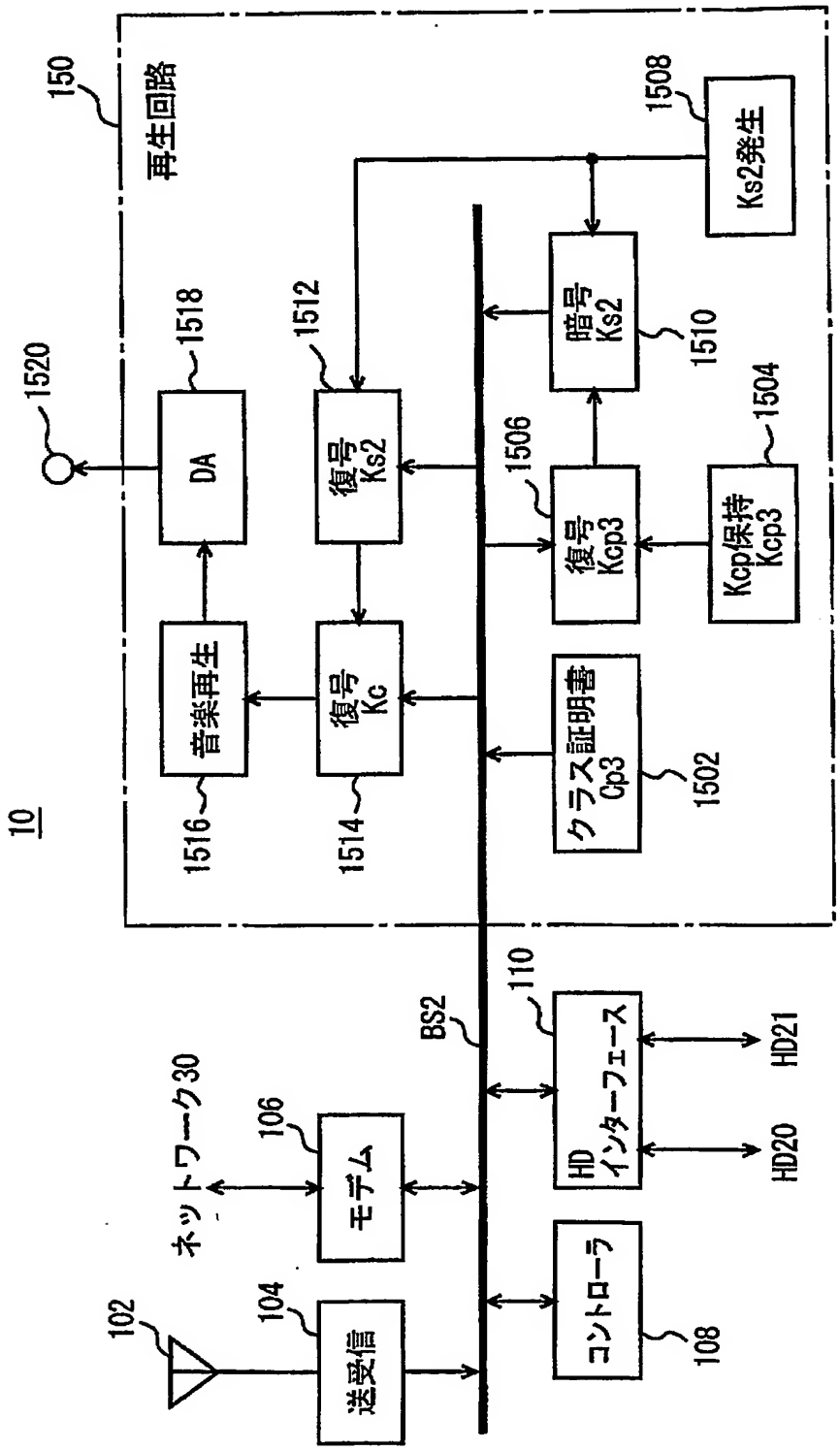
【図３】

	記号	名称	特性
ライセンス提供装置	KPa	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンス提供側にて運用される
	Ks1x	セッション鍵	ライセンスの配信ごとに生成される一時鍵 共通鍵
データ記録装置 (ハードディスク)	Ka	マスタ鍵	クラス証明書作成のために使用する秘密暗号鍵
	KPa	認証鍵	認証局にて証明書を検証する公開復号鍵 認証局にて運用される ライセンス提供側にて運用される
	KPcmy	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
	Kcmy	クラス秘密鍵	クラス公開鍵(KPcmy)にて暗号化されたデータを復号する非対称な復号鍵
	Icmy	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cmy	クラス証明書	Cmy=(KPcmy//Icmy//E(Ka, H(KPcmy//Icmy)) 認証鍵(Ka)によってその正当性が確認できる
	KPomz	個別公開鍵	データ記録装置ごとに固有な値を持つ個別公開暗号鍵 「z」はデータ記録装置を識別するための識別子
	Komz	個別秘密鍵	個別公開鍵(KPomz)にて暗号化されたデータを復号する非対称な復号鍵
	Ks1x	セッション鍵	ライセンスの授受ごとにライセンス提供側で生成される一時鍵 共通鍵
	Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵
再生回路	KPcpy	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
	Kcpy	クラス秘密鍵	クラス公開鍵(KPcpy)にて暗号化されたデータを復号する非対称な復号鍵
	Icpy	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cpy	クラス証明書	Cpy=(KPcpy//Icpy//E(Ka, H(KPcpy//Icpy)) 認証鍵(Ka)によってその正当性が確認できる
	Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵

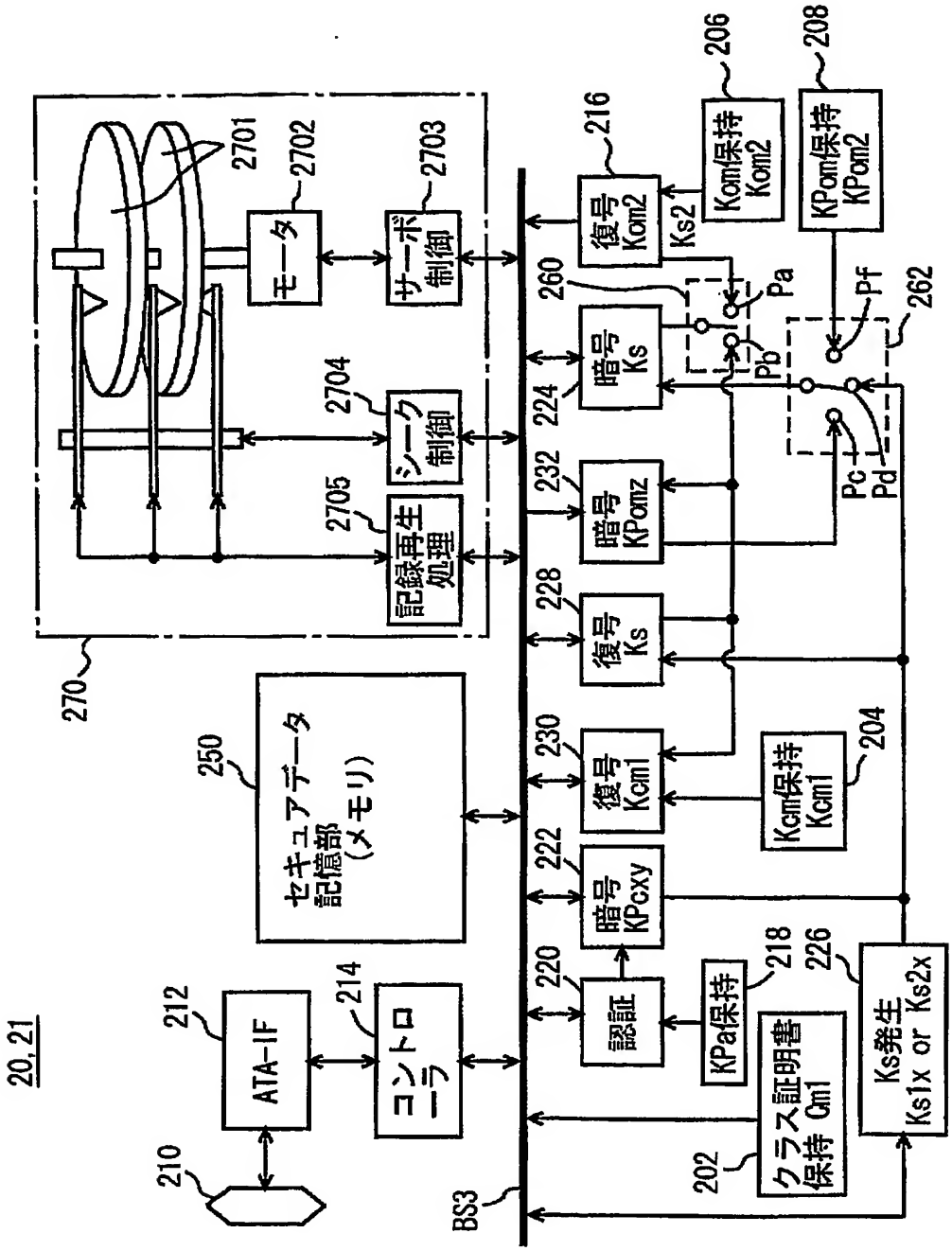
【図４】


40
BS1
ログDB
404
コンテンツDB
402
410
配信制御
412
LIC
暗号化 KPcmz
424
KPcmz
414
Ks発生
Ks1x
暗号化 Ks2
426
Ks2x
復号 Ks1
422
暗号化 KPcmy
420
KPcmy
認証
418
認証鍵 KPa
416
通信装置
450
通信網

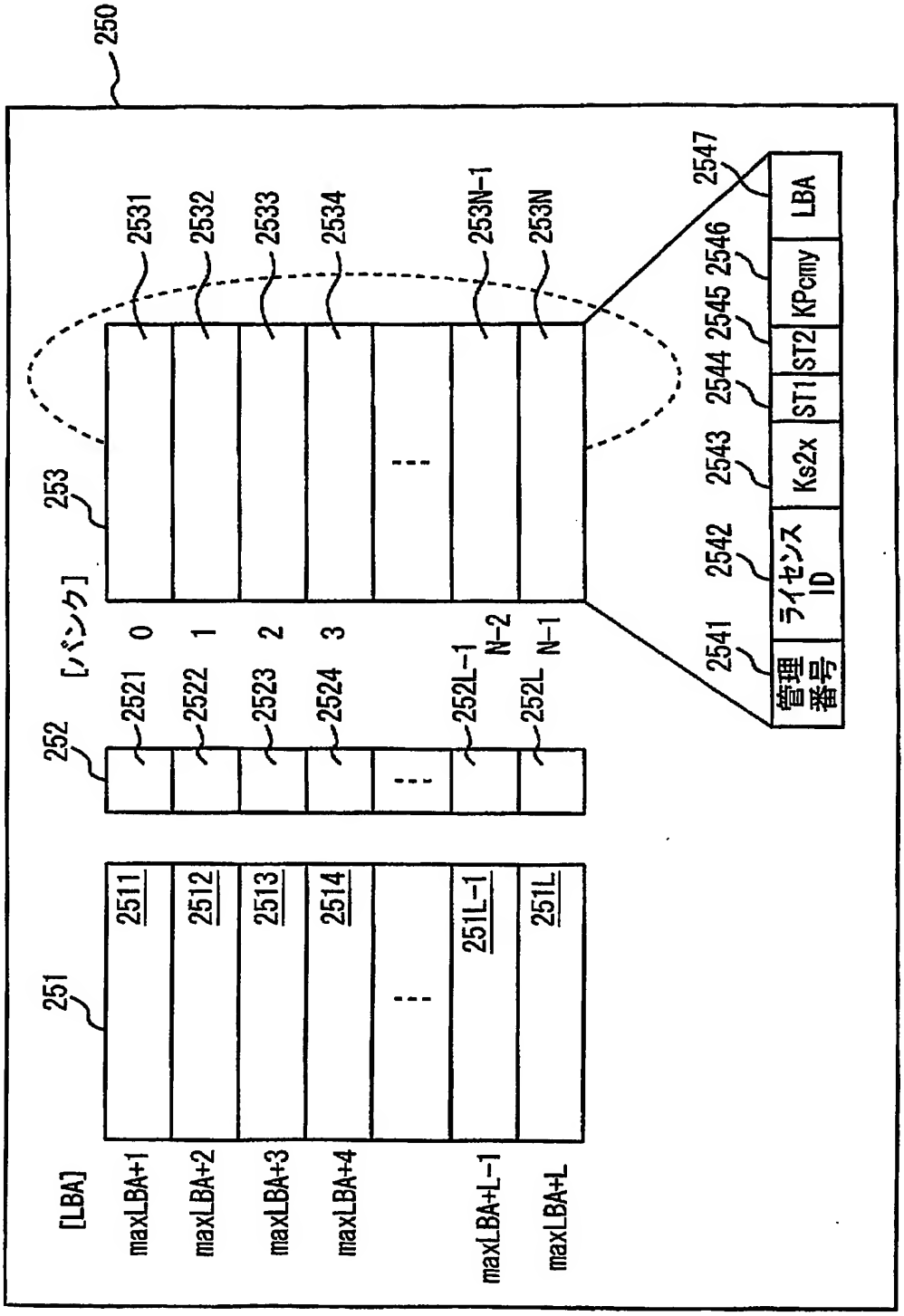
【図５】


10
150
再生回路
1508
Ks2発生
1518
1512
1520
暗号
Ks2
1510
DA
復号
Ks2
1506
1504
復号
Kcp3
Kcp保持
Kcp3
音楽再生
復号
Kc
クラス証明書
Cp3
1502
1516
1514
BS2
110
HD
インターフェース
HD21
HD20
ネットワーク30
106
モデム
102
104
送受信
コントローラ
108

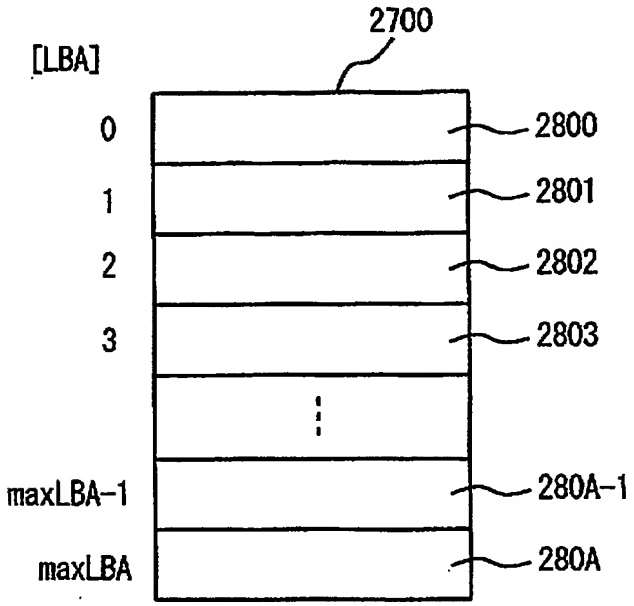
【図６】


20,21
ATA-IF
212
ユントロニラ
214
210
セキュアデータ記憶部（メモリ）
250
270
2701
2702
モータ
2703
サーボ制御
2704
シーク制御
2705
記録再生処理
BS3
認証
220
暗号 KPcxy
222
復号 Kcm1
230
暗号 KPcmz
232
復号 Ks
228
暗号 Ks
224
260
復号 Kcm2
216
Kcm保持 Kcm2
206
KPcm保持 KPcm2
208
Kcm保持 Kcm1
204
KPa保持
218
クラス証明書 保持 Cm1
202
Ks発生 Ks1x or Ks2x
226
Ks2
Pa
Pb
Pc
Pd
Pf
262

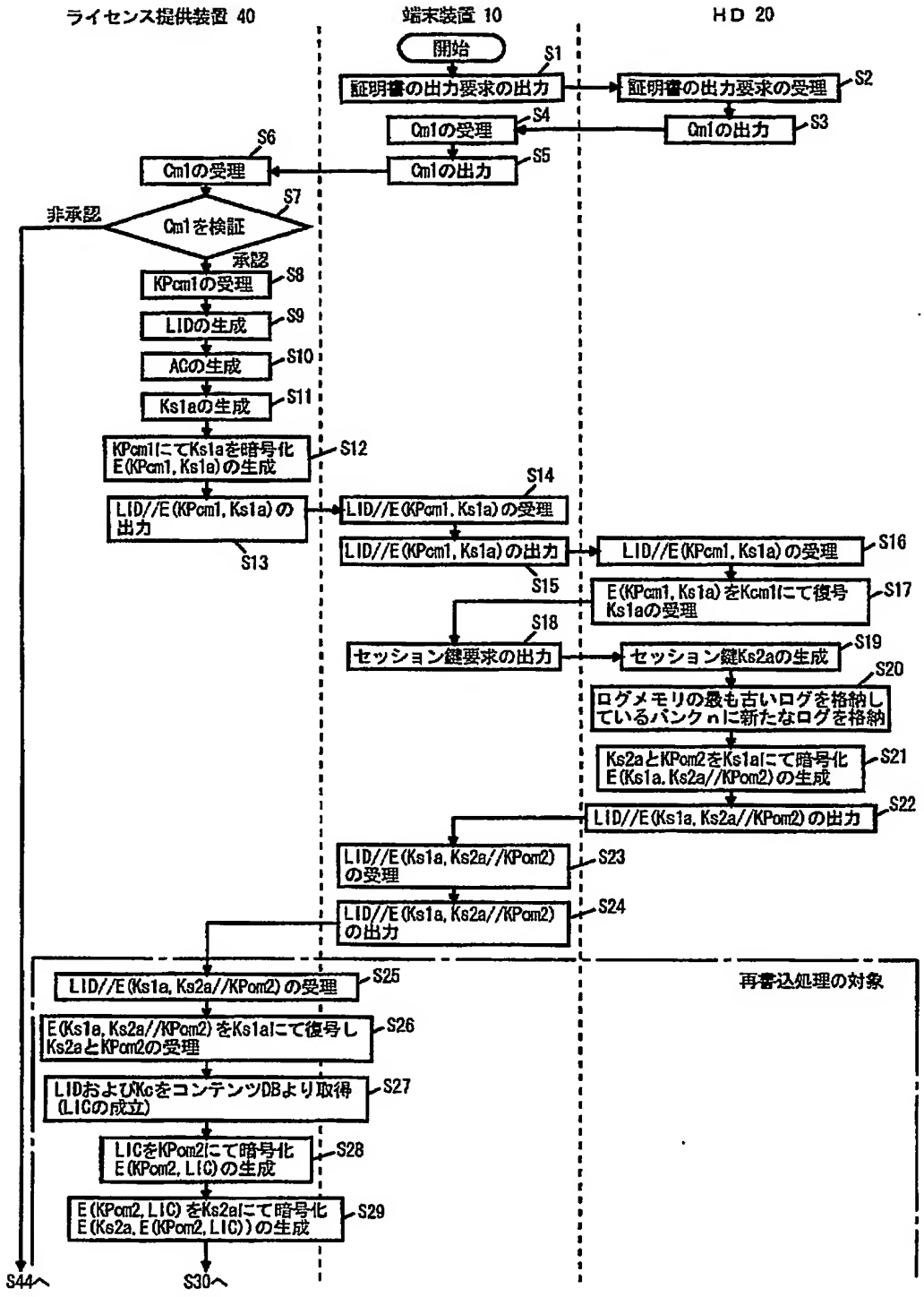
【図７】


250
251
252
253
[LBA]
maxLBA+1
maxLBA+2
maxLBA+3
maxLBA+4
maxLBA+L-1
maxLBA+L
2511
2512
2513
2514
251L-1
251L
[バンク]
2521 0
2522 1
2523 2
2524 3
252L-1 N-2
252L N-1
2531
2532
2533
2534
253N-1
253N
2541 管理番号
2542 ライセンスID
2543 Ks2x
2544 ST1
2545 ST2
2546 KPcmy
2547 LBA

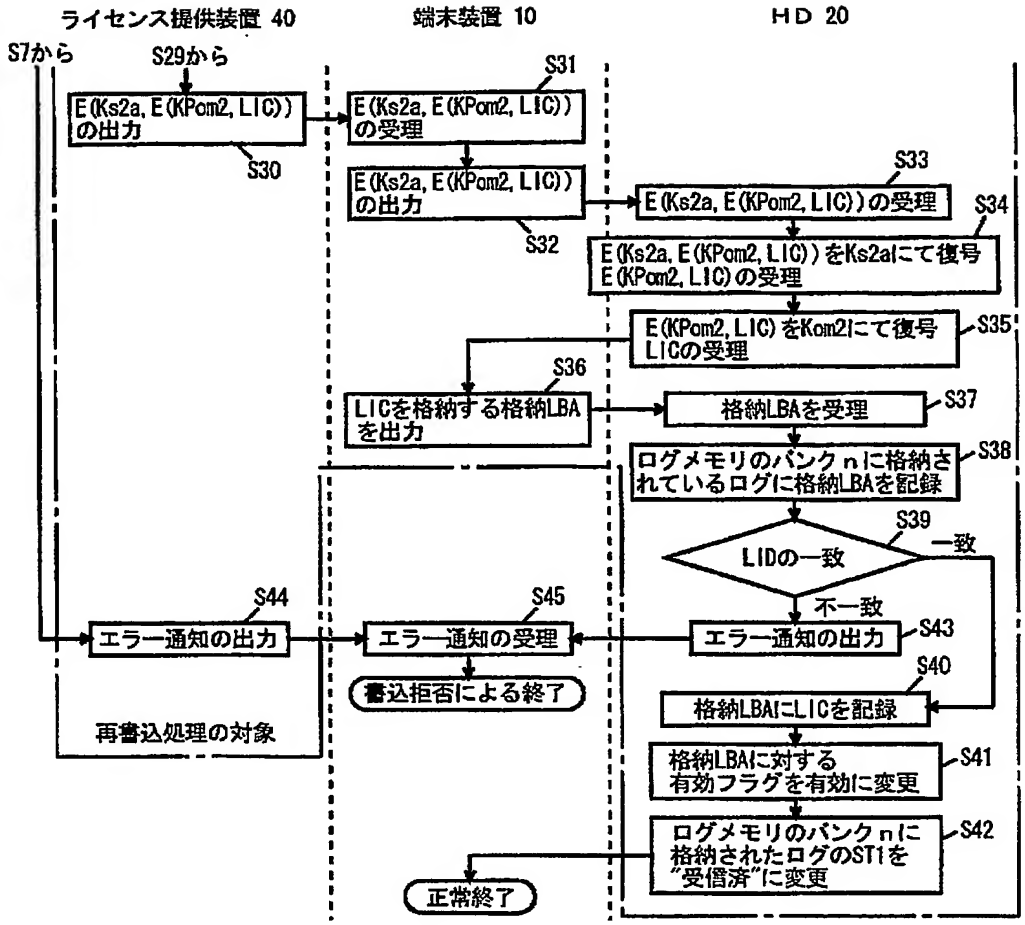
【図８】



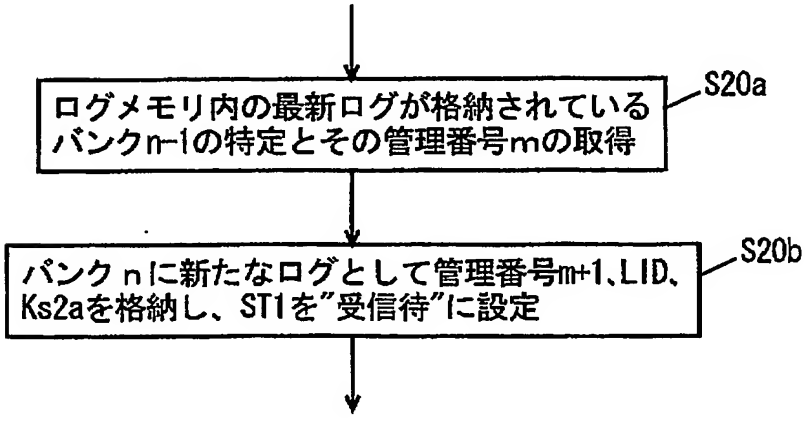
【図９】


ライセンス提供装置 40
端末装置 10
HD 20
開始
S1
証明書の出力要求の出力
S2
証明書の出力要求の受理
S3
Cm1の出力
S4
Cm1の受理
S5
Cm1の出力
S6
Cm1の受理
S7
Cm1を検証
非承認
承認
S8
KPcm1の受理
S9
LIDの生成
S10
ACの生成
S11
Ks1aの生成
S12
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S13
LID//E(KPcm1, Ks1a)の出力
S14
LID//E(KPcm1, Ks1a)の受理
LID//E(KPcm1, Ks1a)の出力
S15
LID//E(KPcm1, Ks1a)の受理
S16
E(KPcm1, Ks1a)をKcm1にて復号
Ks1aの受理
S17
S18
セッション鍵要求の出力
セッション鍵Ks2aの生成
S19
S20
ログメモリの最も古いログを格納しているバンクnに新たなログを格納
Ks2aとKPcm2をKs1aにて暗号化
E(Ks1a, Ks2a//KPcm2)の生成
S21
LID//E(Ks1a, Ks2a//KPcm2)の出力
S22
LID//E(Ks1a, Ks2a//KPcm2)の受理
S23
LID//E(Ks1a, Ks2a//KPcm2)の出力
S24
再書込処理の対象
LID//E(Ks1a, Ks2a//KPcm2)の受理
S25
E(Ks1a, Ks2a//KPcm2)をKs1aにて復号し
Ks2aとKPcm2の受理
S26
LIDおよびKcをコンテンツDBより取得
(LICの成立)
S27
LICをKPcm2にて暗号化
E(KPcm2, LIC)の生成
S28
E(KPcm2, LIC)をKs2aにて暗号化
E(Ks2a, E(KPcm2, LIC))の生成
S29
S44へ
S30へ

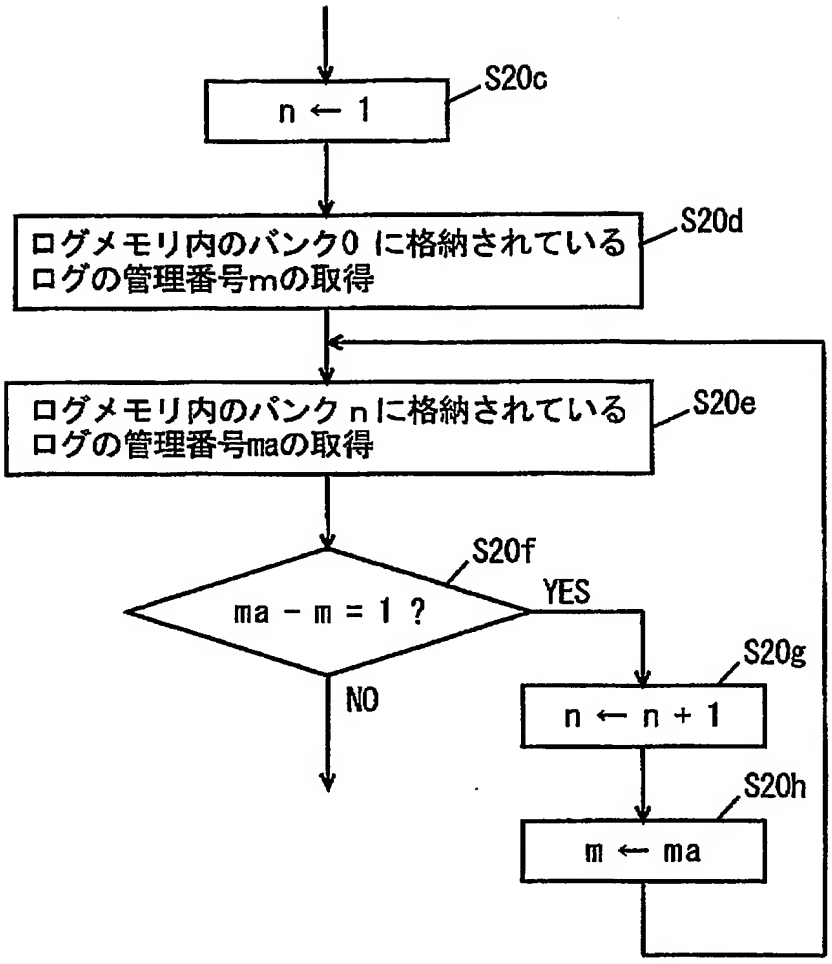
【図１０】


ライセンス提供装置 40
端末装置 10
HD 20
S7から
S29から
E(Ks2a, E(KPom2, LIC))の出力
S30
S31
E(Ks2a, E(KPom2, LIC))の受理
E(Ks2a, E(KPom2, LIC))の出力
S32
S33
E(Ks2a, E(KPom2, LIC))の受理
S34
E(Ks2a, E(KPom2, LIC))をKs2aにて復号
E(KPom2, LIC)の受理
E(KPom2, LIC)をKom2にて復号
LICの受理
S35
S36
LICを格納する格納LBAを出力
格納LBAを受理
S37
ログメモリのバンクｎに格納されているログに格納LBAを記録
S38
S39
LIDの一致
一致
不一致
S44
S45
エラー通知の出力
エラー通知の受理
エラー通知の出力
S43
書込拒否による終了
S40
格納LBAにLICを記録
再書込処理の対象
格納LBAに対する有効フラグを有効に変更
S41
ログメモリのバンクｎに格納されたログのST1を"受信済"に変更
S42
正常終了

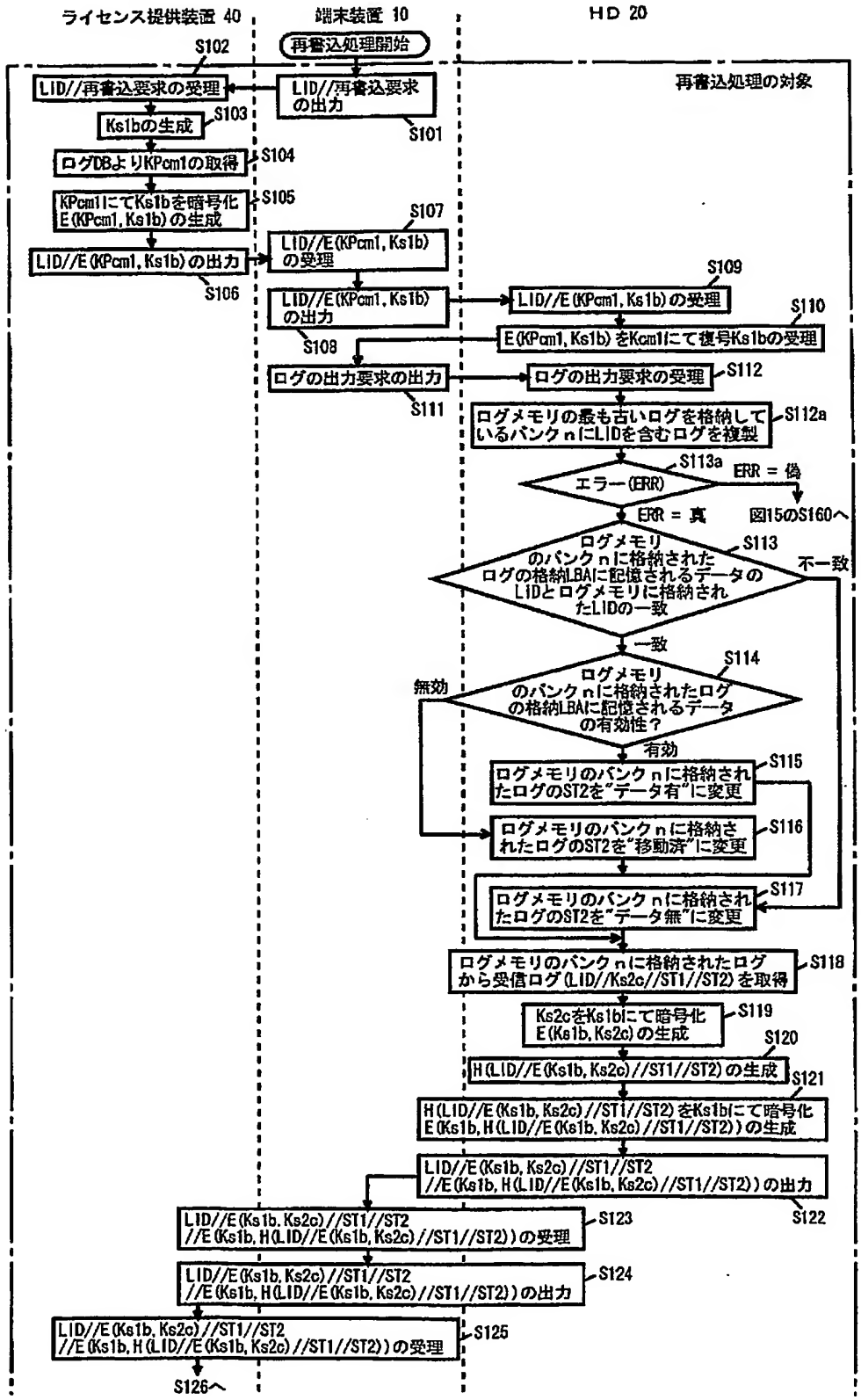
【図１１】


ログメモリ内の最新ログが格納されているバンクn-1の特定とその管理番号mの取得
S20a
バンクｎに新たなログとして管理番号m+1、LID、Ks2aを格納し、ST1を"受信待"に設定
S20b

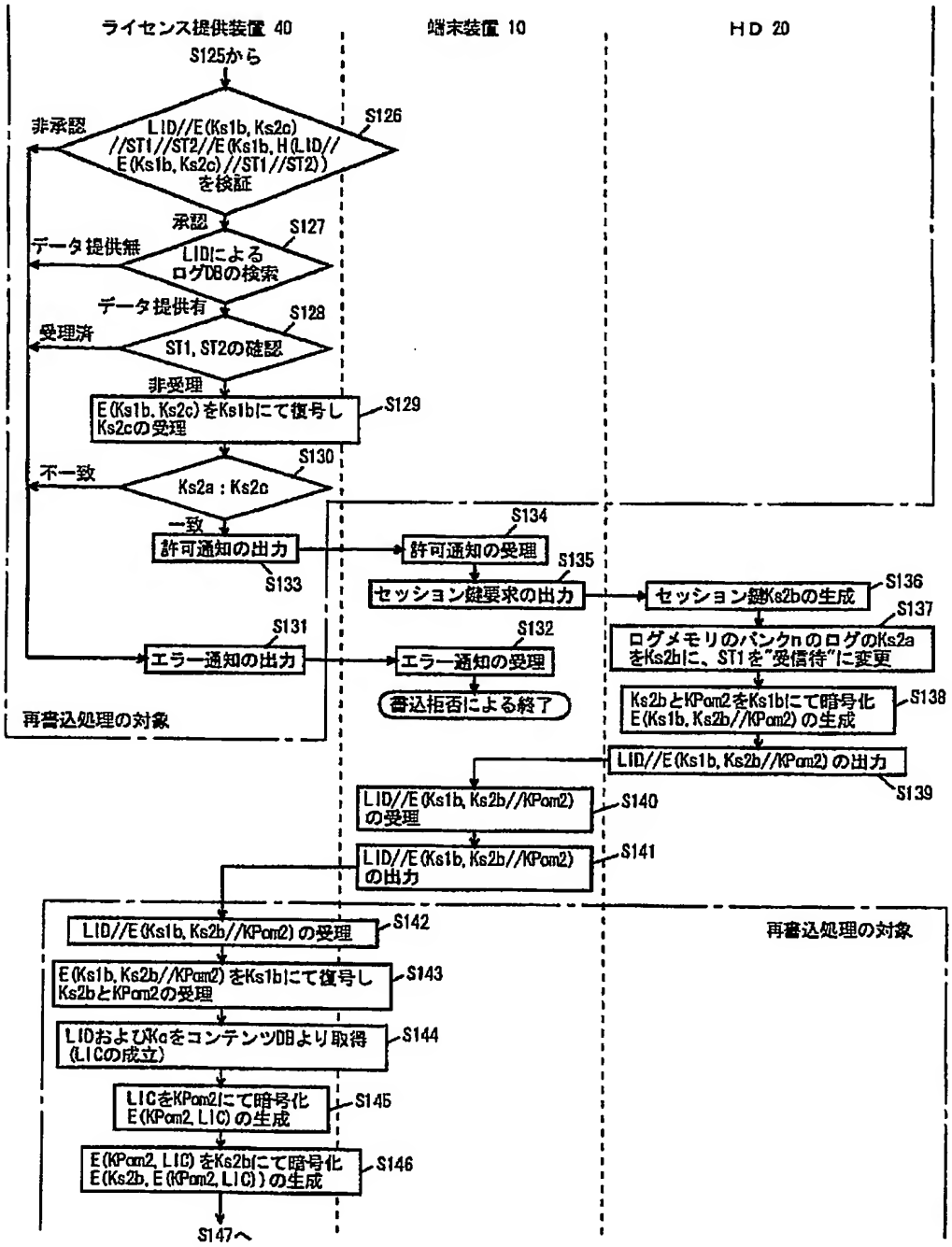
【図１２】


n ← 1
S20c
ログメモリ内のバンク0 に格納されている
ログの管理番号mの取得
S20d
ログメモリ内のバンク n に格納されている
ログの管理番号maの取得
S20e
ma - m = 1 ?
S20f
YES
NO
n ← n + 1
S20g
m ← ma
S20h

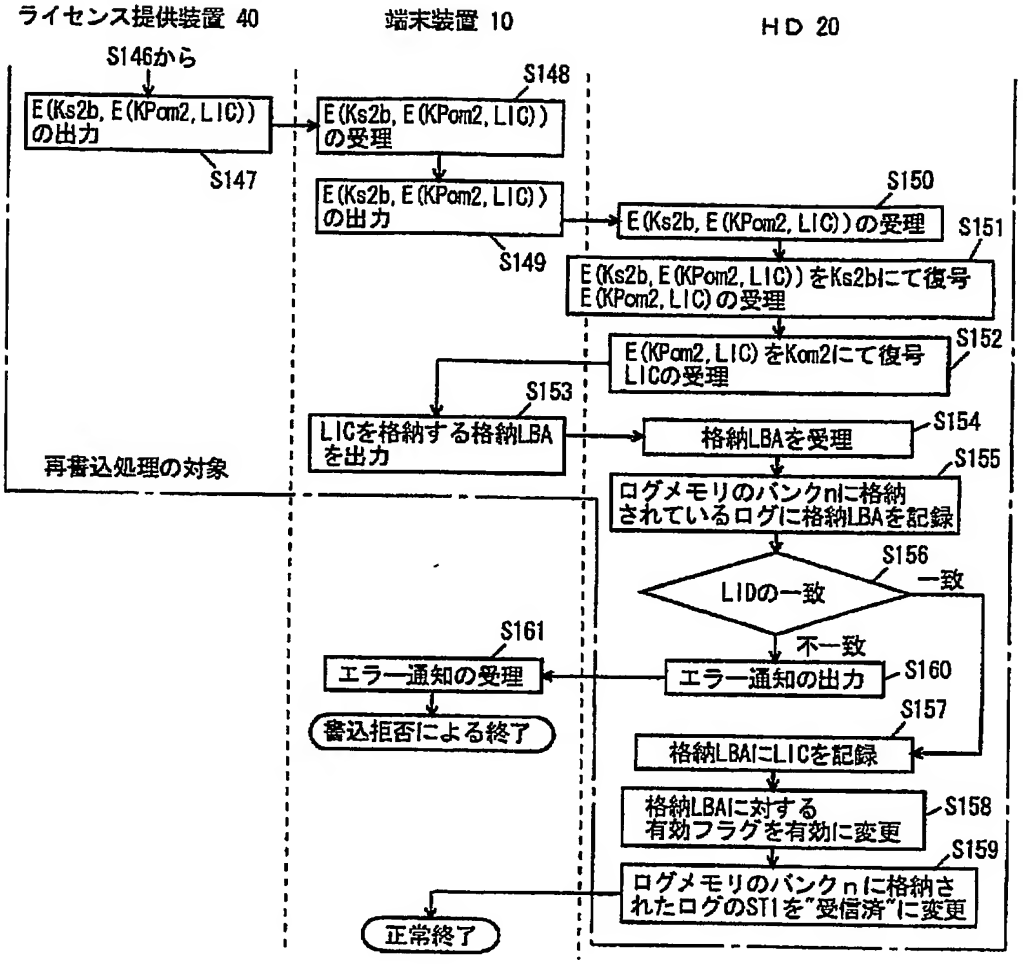
【図１３】


ライセンス提供装置 40
端末装置 10
HD 20
再書込処理の対象
再書込処理開始
S102
LID//再書込要求の受理
LID//再書込要求の出力
S101
S103
Ks1bの生成
S104
ログDBよりKPcm1の取得
S105
KPcm1にてKs1bを暗号化 E(KPcm1, Ks1b)の生成
S107
LID//E(KPcm1, Ks1b)の受理
LID//E(KPcm1, Ks1b)の出力
S106
S109
LID//E(KPcm1, Ks1b)の受理
S110
E(KPcm1, Ks1b)をKcm1にて復号Ks1bの受理
S108
ログの出力要求の出力
ログの出力要求の受理
S112
S111
S112a
ログメモリの最も古いログを格納しているバンクnにLIDを含むログを複製
S113a
エラー(ERR)
ERR = 偽
ERR = 真
図15のS160へ
S113
ログメモリのバンクnに格納されたログの格納LBAに記憶されるデータのLIDとログメモリに格納されたLIDの一致
不一致
一致
S114
ログメモリのバンクnに格納されたログの格納LBAに記憶されるデータの有効性？
無効
有効
S115
ログメモリのバンクnに格納されたログのST2を"データ有"に変更
S116
ログメモリのバンクnに格納されたログのST2を"移動済"に変更
S117
ログメモリのバンクnに格納されたログのST2を"データ無"に変更
S118
ログメモリのバンクnに格納されたログから受信ログ(LID//Ks2c//ST1//ST2)を取得
S119
Ks2cをKs1bにて暗号化 E(Ks1b, Ks2c)の生成
S120
H(LID//E(Ks1b, Ks2c)//ST1//ST2)の生成
S121
H(LID//E(Ks1b, Ks2c)//ST1//ST2)をKs1bにて暗号化 E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の生成
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S122
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S123
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S124
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S125
S126へ

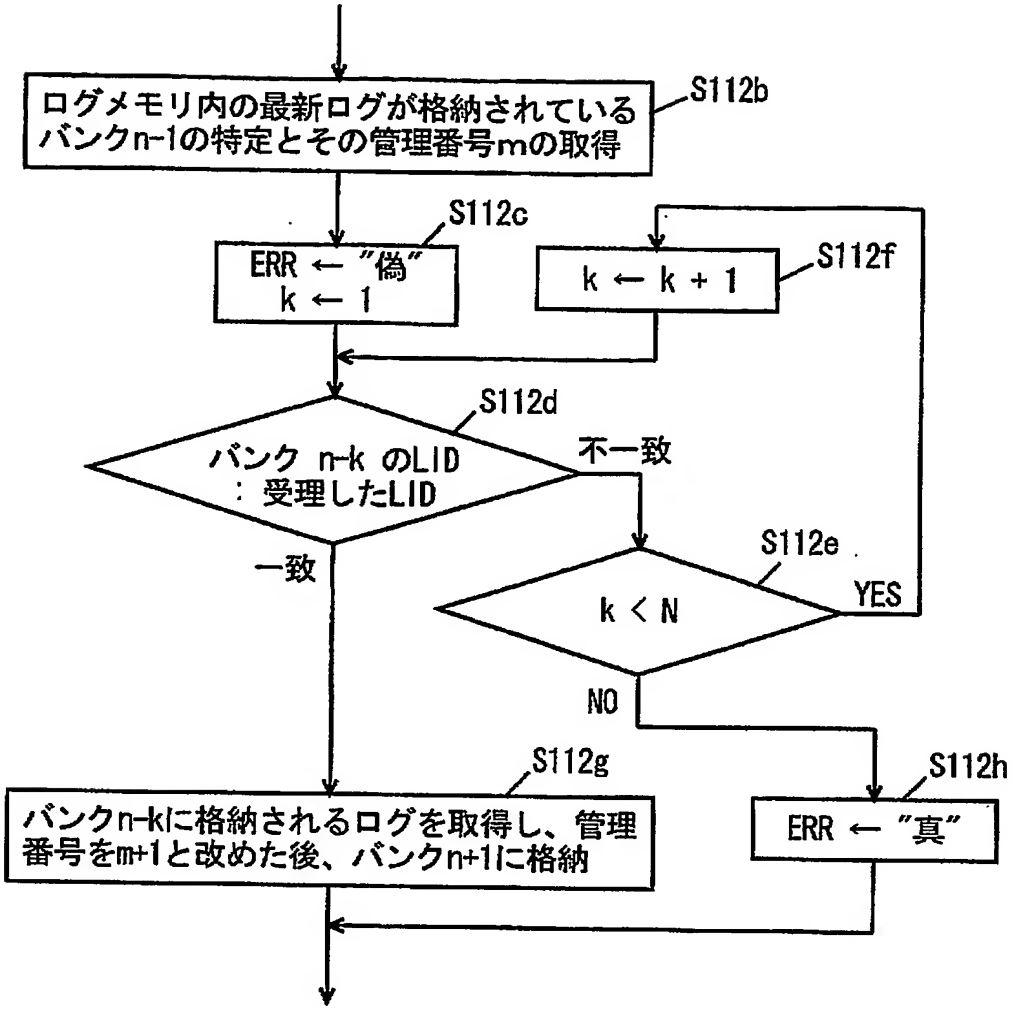
【図１４】


ライセンス提供装置 40
端末装置 10
HD 20
S125から
S126
LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を検証
非承認
承認
S127
データ提供無
LIDによるログDBの検索
データ提供有
S128
受理済
ST1, ST2の確認
非受理
S129
E(Ks1b, Ks2c)をKs1bにて復号しKs2cの受理
S130
不一致
Ks2a : Ks2c
一致
許可通知の出力
S133
S134
許可通知の受理
S135
セッション鍵要求の出力
S136
セッション鍵Ks2bの生成
S137
ログメモリのバンクnのログのKs2aをKs2bに、ST1を"受信待"に変更
S131
エラー通知の出力
S132
エラー通知の受理
書込拒否による終了
再書込処理の対象
S138
Ks2bとKPam2をKs1bにて暗号化E(Ks1b, Ks2b//KPam2)の生成
LID//E(Ks1b, Ks2b//KPam2)の出力
S139
LID//E(Ks1b, Ks2b//KPam2)の受理
S140
LID//E(Ks1b, Ks2b//KPam2)の出力
S141
LID//E(Ks1b, Ks2b//KPam2)の受理
S142
再書込処理の対象
E(Ks1b, Ks2b//KPam2)をKs1bにて復号しKs2bとKPam2の受理
S143
LIDおよびKcをコンテンツDBより取得(LICの成立)
S144
LICをKPam2にて暗号化E(KPam2, LIC)の生成
S145
E(KPam2, LIC)をKs2bにて暗号化E(Ks2b, E(KPam2, LIC))の生成
S146
S147へ

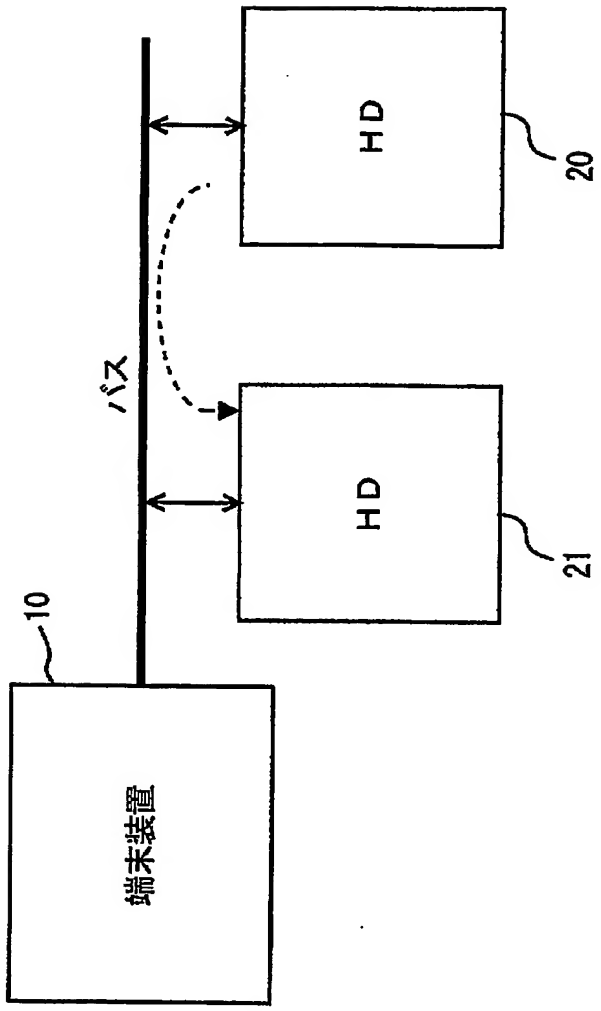
【図１５】


ライセンス提供装置 40
端末装置 10
HD 20
S146から
E(Ks2b, E(KPom2, LIC))の出力
S147
S148
E(Ks2b, E(KPom2, LIC))の受理
E(Ks2b, E(KPom2, LIC))の出力
S149
S150
E(Ks2b, E(KPom2, LIC))の受理
S151
E(Ks2b, E(KPom2, LIC))をKs2bにて復号
E(KPom2, LIC)の受理
E(KPom2, LIC)をKom2にて復号
LICの受理
S152
S153
LICを格納する格納LBAを出力
格納LBAを受理
S154
S155
ログメモリのバンクnに格納されているログに格納LBAを記録
S156
LIDの一致
一致
不一致
S161
エラー通知の受理
エラー通知の出力
S160
書込拒否による終了
S157
格納LBAにLICを記録
格納LBAに対する有効フラグを有効に変更
S158
S159
ログメモリのバンクｎに格納されたログのST1を"受信済"に変更
正常終了
再書込処理の対象

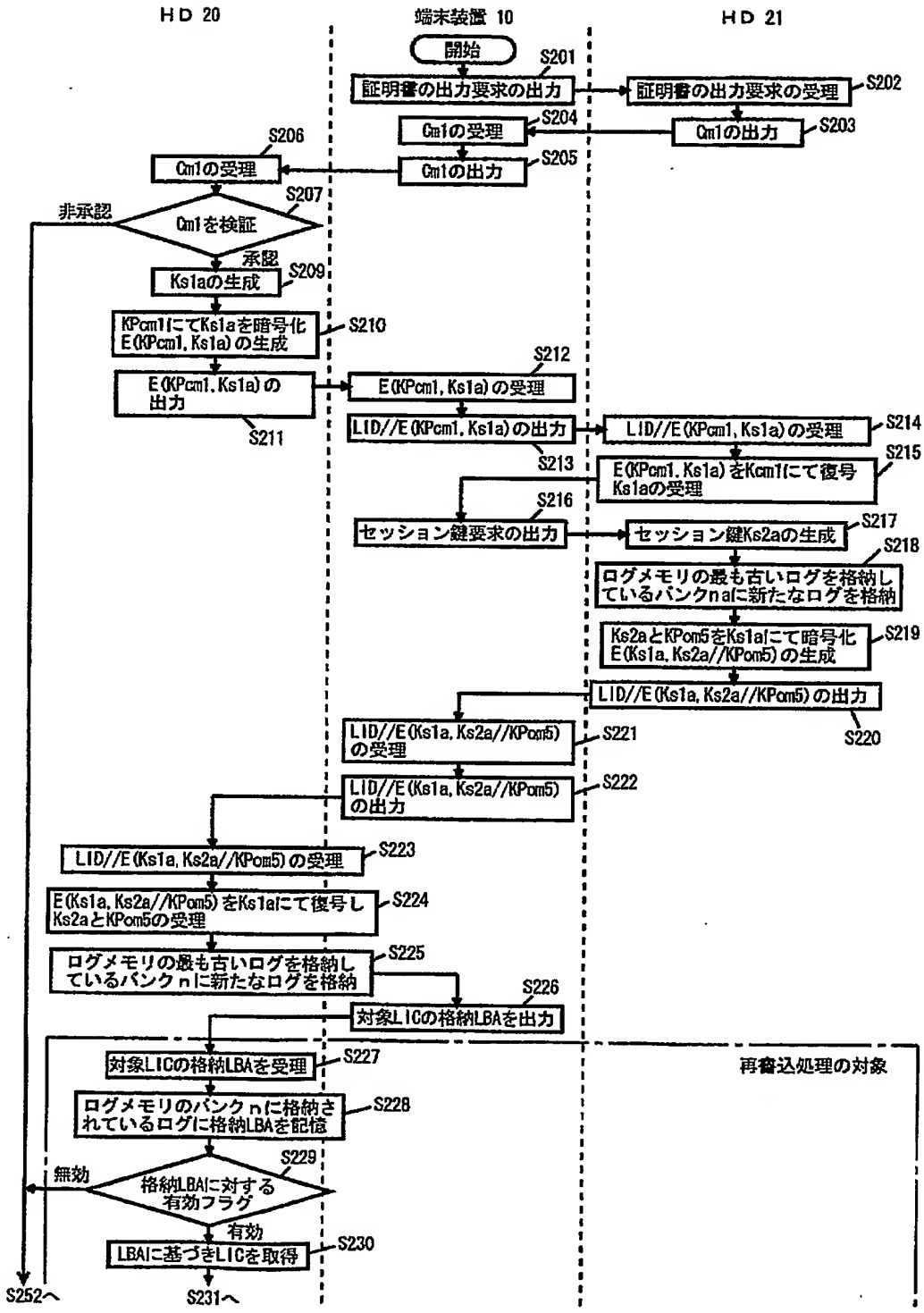
【図１６】


ログメモリ内の最新ログが格納されている
バンクn-1の特定とその管理番号mの取得
S112b
ERR ← "偽"
k ← 1
S112c
k ← k + 1
S112f
バンク n-k のLID
：受理したLID
S112d
不一致
一致
k < N
S112e
YES
NO
バンクn-kに格納されるログを取得し、管理
番号をm+1と改めた後、バンクn+1に格納
S112g
ERR ← "真"
S112h

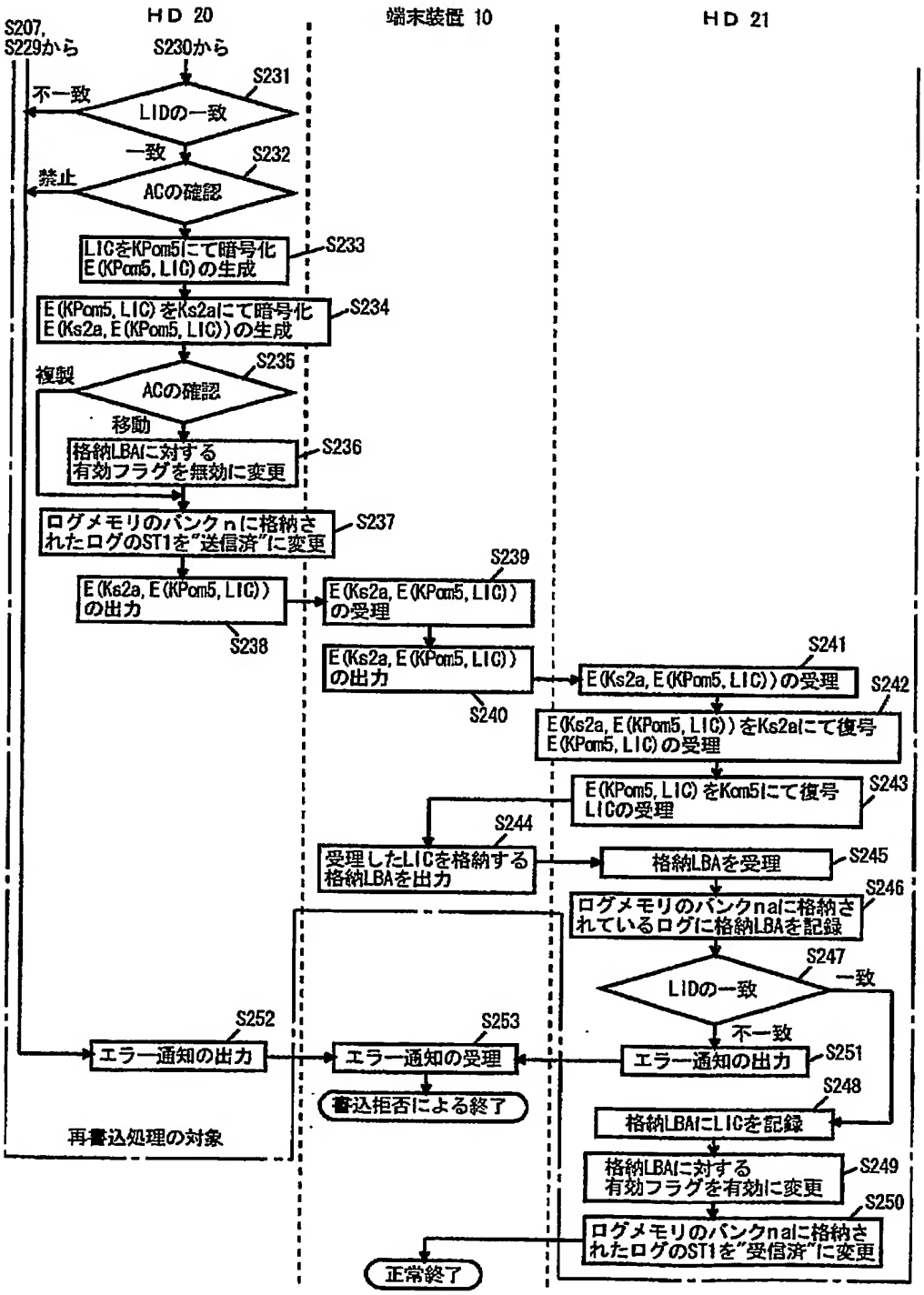
【図１７】



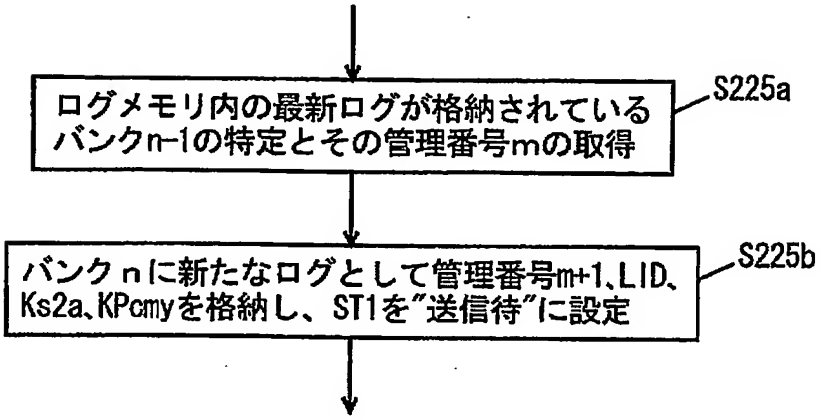
【図１８】


HD 20
端末装置 10
HD 21
開始
S201
証明書の出力要求の出力
証明書の出力要求の受理
S202
Cm1の受理
S204
Cm1の出力
S203
S206
Cm1の受理
Cm1の出力
S205
S207
非承認
Cm1を検証
承認
Ks1aの生成
S209
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S210
S212
E(KPcm1, Ks1a)の
出力
E(KPcm1, Ks1a)の受理
S211
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S214
S213
E(KPcm1, Ks1a)をKcm1にて復号
Ks1aの受理
S215
S216
セッション鍵要求の出力
セッション鍵Ks2aの生成
S217
S218
ログメモリの最も古いログを格納し
ているバンクnaに新たなログを格納
Ks2aとKPom5をKs1aにて暗号化
E(Ks1a, Ks2a//KPom5)の生成
S219
LID//E(Ks1a, Ks2a//KPom5)の出力
S220
LID//E(Ks1a, Ks2a//KPom5)
の受理
S221
LID//E(Ks1a, Ks2a//KPom5)
の出力
S222
LID//E(Ks1a, Ks2a//KPom5)の受理
S223
E(Ks1a, Ks2a//KPom5)をKs1aにて復号し
Ks2aとKPom5の受理
S224
ログメモリの最も古いログを格納し
ているバンクｎに新たなログを格納
S225
S226
対象LICの格納LBAを出力
再書込処理の対象
対象LICの格納LBAを受理
S227
ログメモリのバンクｎに格納さ
れているログに格納LBAを記憶
S228
S229
無効
格納LBAに対する
有効フラグ
有効
LBAに基づきLICを取得
S230
S252へ
S231へ

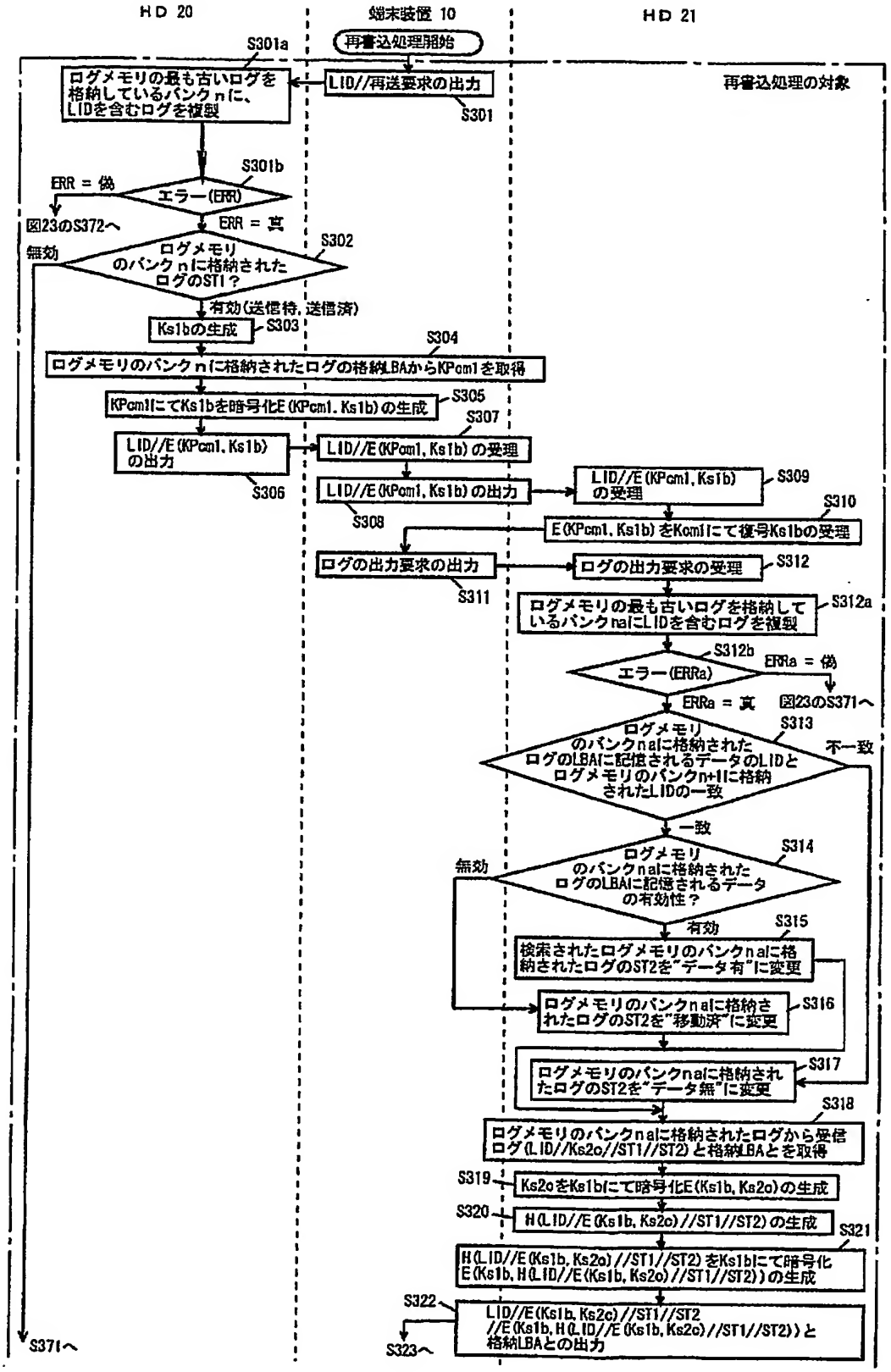
【図１９】


HD 20
端末装置 10
HD 21
S207,
S229から
S230から
S231
不一致
LIDの一致
一致
S232
禁止
ACの確認
LICをKPom5にて暗号化
E(KPom5, LIC)の生成
S233
E(KPom5, LIC)をKs2aにて暗号化
E(Ks2a, E(KPom5, LIC))の生成
S234
S235
複製
ACの確認
移動
格納LBAに対する
有効フラグを無効に変更
S236
ログメモリのバンクｎに格納さ
れたログのST1を"送信済"に変更
S237
S239
E(Ks2a, E(KPom5, LIC))
の出力
S238
E(Ks2a, E(KPom5, LIC))
の受理
E(Ks2a, E(KPom5, LIC))
の出力
S240
S241
E(Ks2a, E(KPom5, LIC))の受理
S242
E(Ks2a, E(KPom5, LIC))をKs2aにて復号
E(KPom5, LIC)の受理
E(KPom5, LIC)をKom5にて復号
LICの受理
S243
S244
受理したLICを格納する
格納LBAを出力
格納LBAを受理
S245
ログメモリのバンクnaに格納さ
れているログに格納LBAを記録
S246
S247
LIDの一致
一致
不一致
S252
S253
エラー通知の出力
エラー通知の受理
エラー通知の出力
S251
書込拒否による終了
S248
格納LBAにLICを記録
再書込処理の対象
格納LBAに対する
有効フラグを有効に変更
S249
S250
ログメモリのバンクnaに格納さ
れたログのST1を"受信済"に変更
正常終了

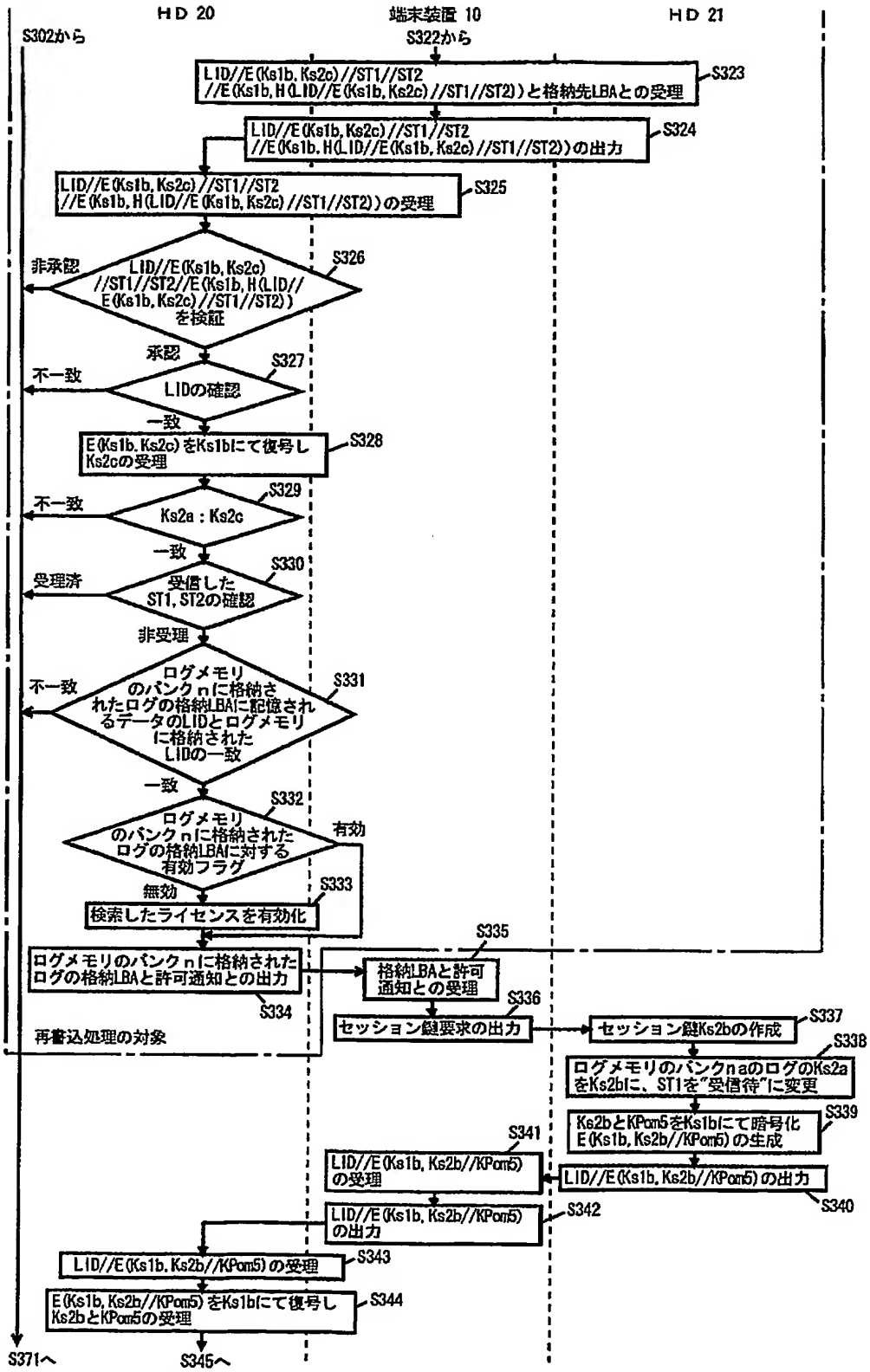
【図２０】


ログメモリ内の最新ログが格納されている
バンクn-1の特定とその管理番号mの取得
S225a
バンクｎに新たなログとして管理番号m+1、LID、
Ks2a、KPcmyを格納し、ST1を"送信待"に設定
S225b

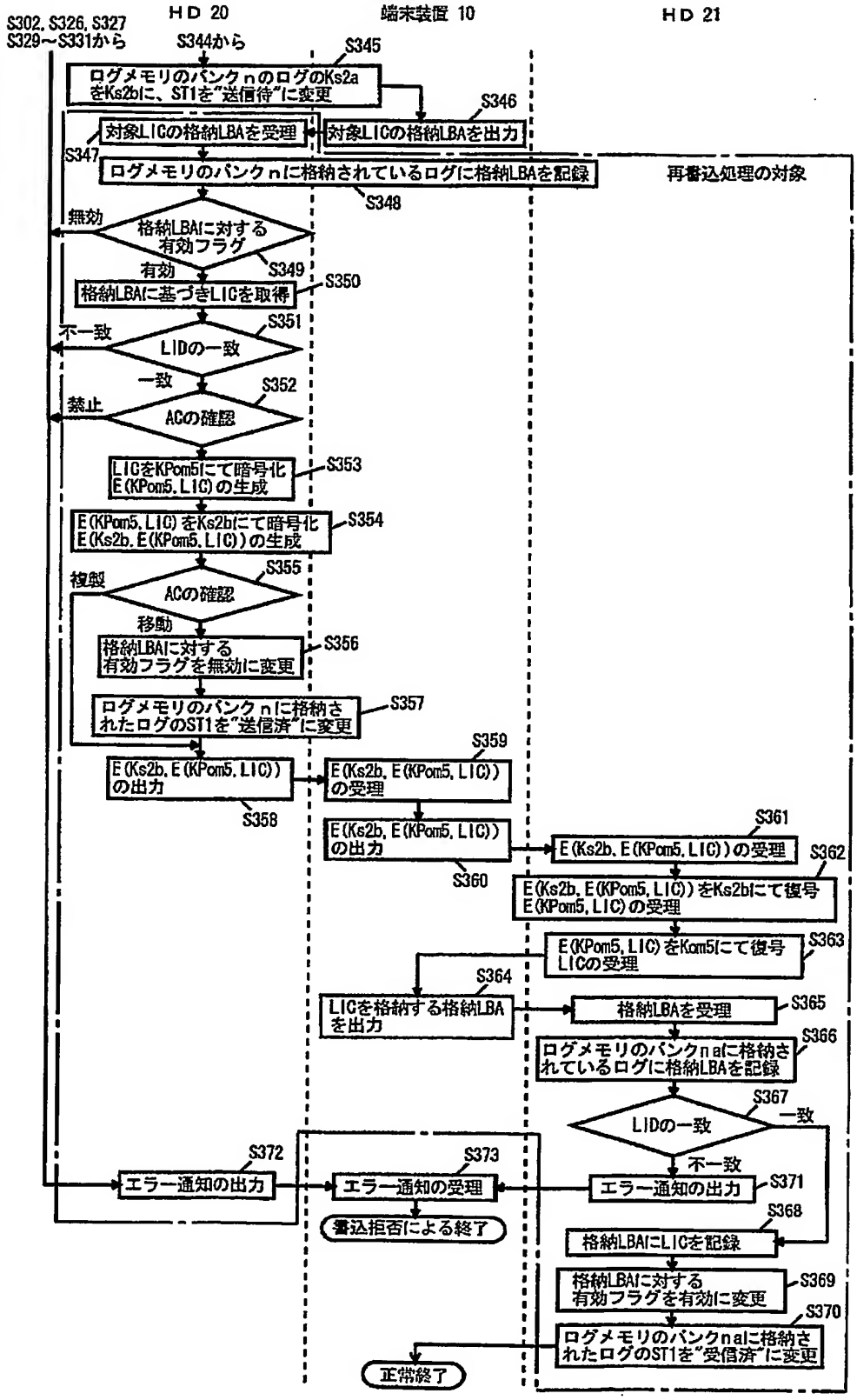
【図２１】


HD 20
端末装置 10
HD 21
再書込処理開始
S301a
ログメモリの最も古いログを格納しているバンクｎに、LIDを含むログを複製
LID//再送要求の出力
S301
再書込処理の対象
S301b
ERR = 偽
エラー(ERR)
ERR = 真
図23のS372へ
S302
無効
ログメモリのバンクｎに格納されたログのST1？
有効(送信待，送信済)
Ks1bの生成
S303
S304
ログメモリのバンクｎに格納されたログの格納LBAからKPcm1を取得
KPcm1にてKs1bを暗号化E(KPcm1, Ks1b)の生成
S305
LID//E(KPcm1, Ks1b)の出力
S306
S307
LID//E(KPcm1, Ks1b)の受理
LID//E(KPcm1, Ks1b)の出力
S308
LID//E(KPcm1, Ks1b)の受理
S309
E(KPcm1, Ks1b)をKcm1にて復号Ks1bの受理
S310
ログの出力要求の出力
S311
ログの出力要求の受理
S312
ログメモリの最も古いログを格納しているバンクnaにLIDを含むログを複製
S312a
S312b
エラー(ERRa)
ERRa = 偽
図23のS371へ
ERRa = 真
S313
ログメモリのバンクnaに格納されたログのLBAに記憶されるデータのLIDとログメモリのバンクn+1に格納されたLIDの一致
不一致
一致
S314
無効
ログメモリのバンクnaに格納されたログのLBAに記憶されるデータの有効性？
有効
S315
検索されたログメモリのバンクnaに格納されたログのST2を"データ有"に変更
ログメモリのバンクnaに格納されたログのST2を"移動済"に変更
S316
ログメモリのバンクnaに格納されたログのST2を"データ無"に変更
S317
S318
ログメモリのバンクnaに格納されたログから受信ログ(LID//Ks2o//ST1//ST2)と格納LBAとを取得
S319
Ks2oをKs1bにて暗号化E(Ks1b, Ks2o)の生成
S320
H(LID//E(Ks1b, Ks2o)//ST1//ST2)の生成
S321
H(LID//E(Ks1b, Ks2o)//ST1//ST2)をKs1bにて暗号化E(Ks1b, H(LID//E(Ks1b, Ks2o)//ST1//ST2))の生成
S322
LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))と格納LBAとの出力
S323へ
S371へ

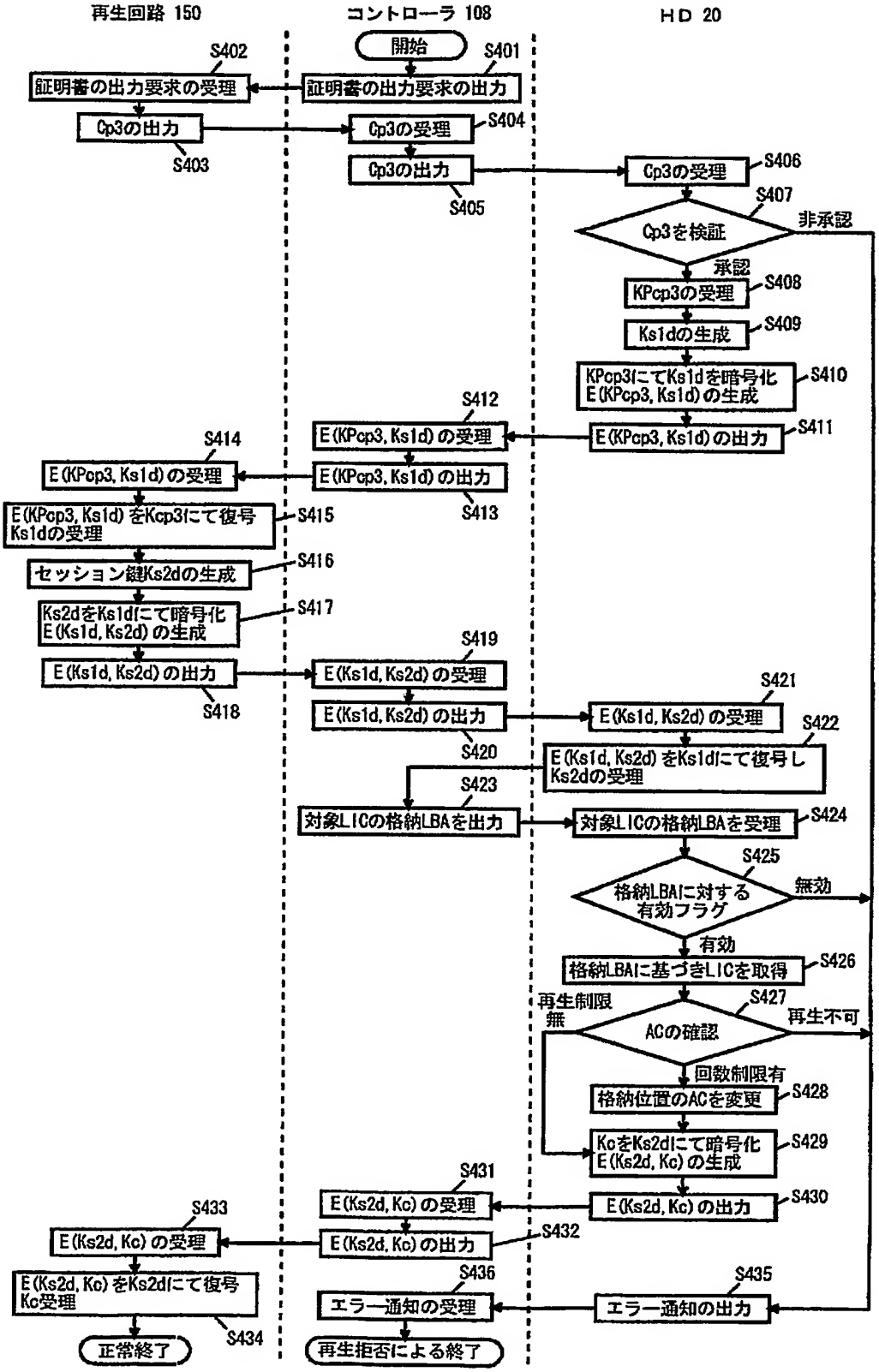
【図２２】


HD 20
端末装置 10
HD 21
S302から
S322から
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))と格納先LBAとの受理
S323
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S324
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S325
非承認
LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を検証
S326
承認
不一致
LIDの確認
S327
一致
E(Ks1b, Ks2c)をKs1bにて復号しKs2cの受理
S328
不一致
Ks2a：Ks2c
S329
一致
受理済
受信したST1, ST2の確認
S330
非受理
不一致
ログメモリのバンクnに格納されたログの格納LBAに記憶されるデータのLIDとログメモリに格納されたLIDの一致
S331
一致
ログメモリのバンクnに格納されたログの格納LBAに対する有効フラグ
S332
有効
無効
検索したライセンスを有効化
S333
S335
ログメモリのバンクnに格納されたログの格納LBAと許可通知との出力
S334
格納LBAと許可通知との受理
S336
セッション鍵要求の出力
S337
セッション鍵Ks2bの作成
S338
ログメモリのバンクnaのログのKs2aをKs2bに、ST1を"受信待"に変更
S339
Ks2bとKPam5をKs1bにて暗号化E(Ks1b, Ks2b//KPam5)の生成
S341
LID//E(Ks1b, Ks2b//KPam5)の受理
LID//E(Ks1b, Ks2b//KPam5)の出力
S340
LID//E(Ks1b, Ks2b//KPam5)の出力
S342
LID//E(Ks1b, Ks2b//KPam5)の受理
S343
E(Ks1b, Ks2b//KPam5)をKs1bにて復号しKs2bとKPam5の受理
S344
再書込処理の対象
S371へ
S345へ

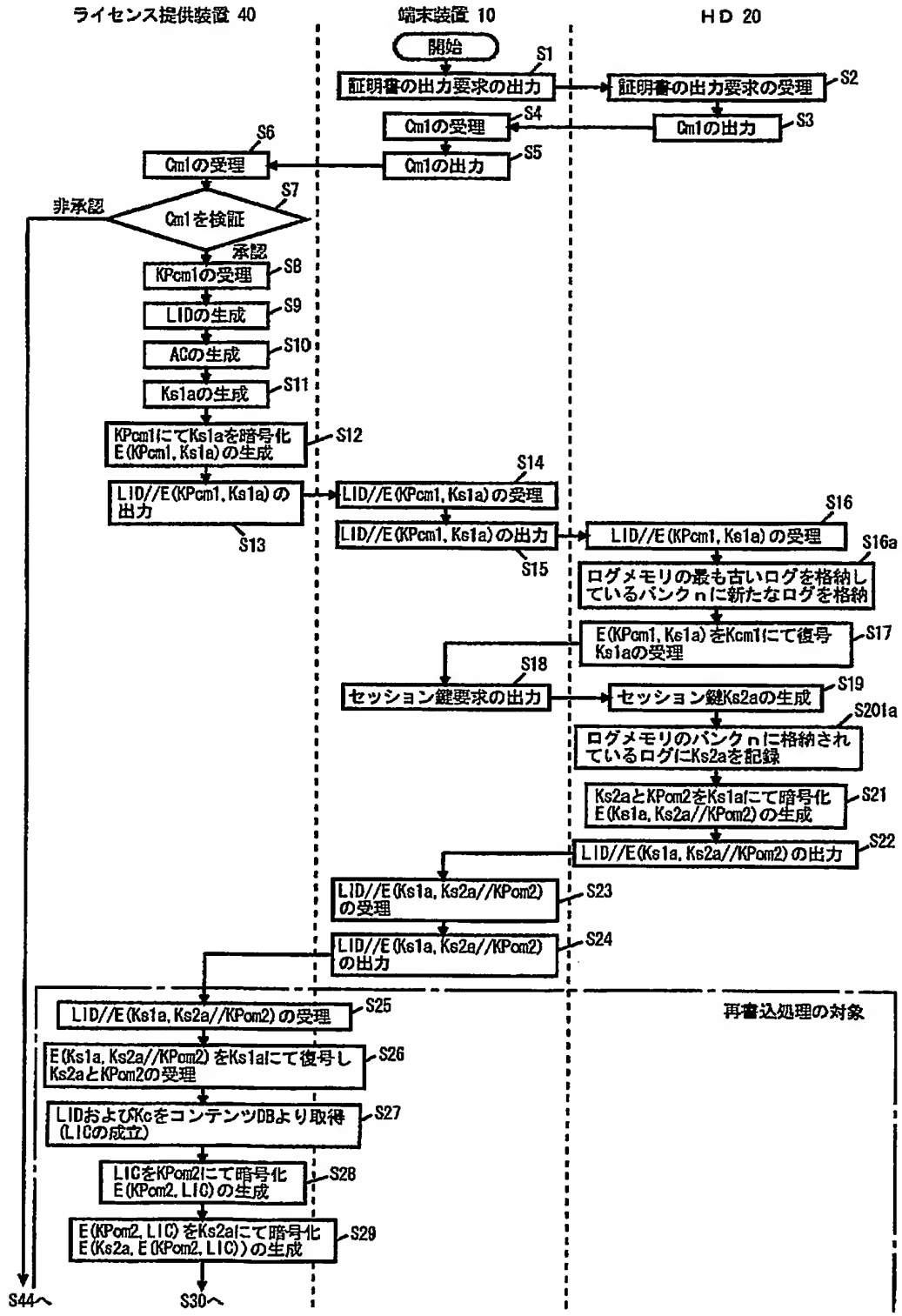
【図２３】


HD 20
端末装置 10
HD 21
S302, S326, S327
S329～S331から
S344から
S345
ログメモリのバンクｎのログのKs2a
をKs2bに、ST1を"送信待"に変更
S346
対象LICの格納LBAを受理
対象LICの格納LBAを出力
S347
ログメモリのバンクｎに格納されているログに格納LBAを記録
再書込処理の対象
S348
無効
格納LBAに対する
有効フラグ
S349
有効
格納LBAに基づきLICを取得
S350
不一致
S351
LIDの一致
一致
S352
禁止
ACの確認
LICをKPom5にて暗号化
E(KPom5, LIC)の生成
S353
E(KPom5, LIC)をKs2bにて暗号化
E(Ks2b, E(KPom5, LIC))の生成
S354
複製
S355
ACの確認
移動
格納LBAに対する
有効フラグを無効に変更
S356
ログメモリのバンクｎに格納さ
れたログのST1を"送信済"に変更
S357
E(Ks2b, E(KPom5, LIC))
の出力
S358
S359
E(Ks2b, E(KPom5, LIC))
の受理
E(Ks2b, E(KPom5, LIC))
の出力
S360
S361
E(Ks2b, E(KPom5, LIC))の受理
S362
E(Ks2b, E(KPom5, LIC))をKs2bにて復号
E(KPom5, LIC)の受理
E(KPom5, LIC)をKom5にて復号
LICの受理
S363
S364
LICを格納する格納LBA
を出力
格納LBAを受理
S365
ログメモリのバンクｎaに格納さ
れているログに格納LBAを記録
S366
S367
LIDの一致
一致
不一致
S372
エラー通知の出力
S373
エラー通知の受理
エラー通知の出力
S371
書込拒否による終了
S368
格納LBAにLICを記録
格納LBAに対する
有効フラグを有効に変更
S369
S370
ログメモリのバンクｎaに格納さ
れたログのST1を"受信済"に変更
正常終了

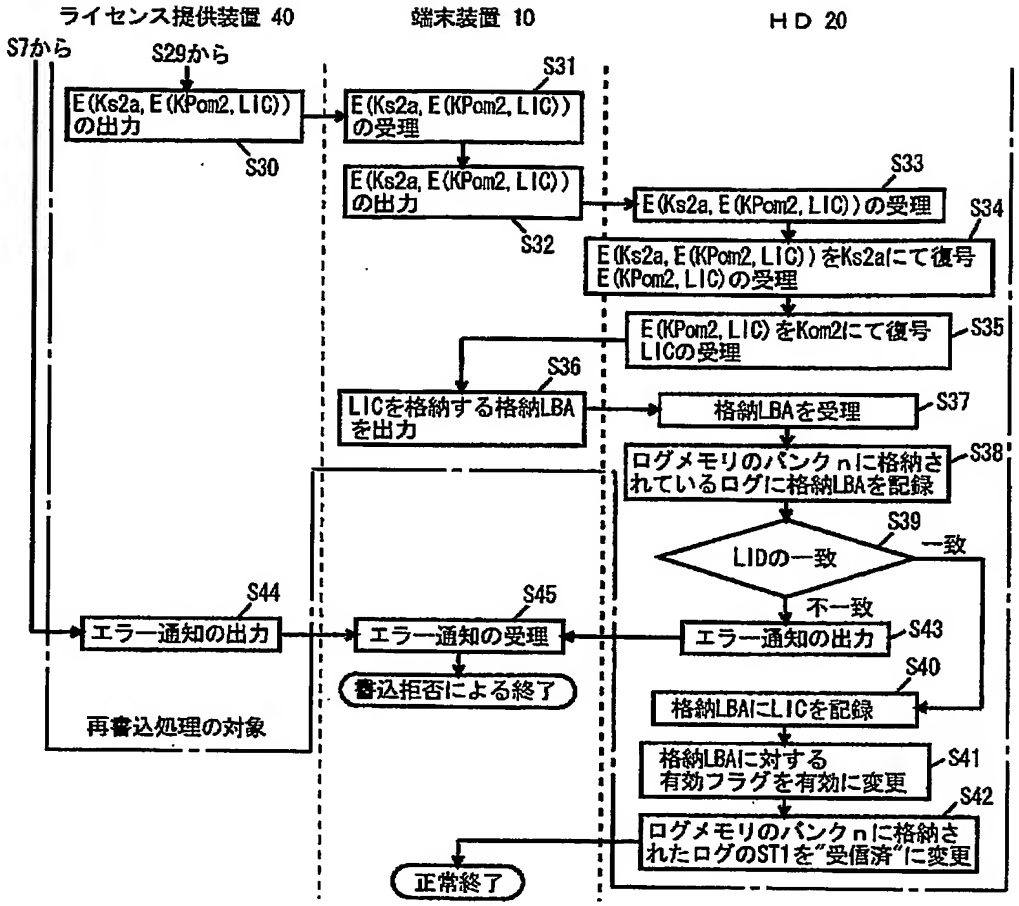
【図２４】


再生回路 150
コントローラ 108
HD 20
開始
S401
証明書の出力要求の出力
S402
証明書の出力要求の受理
Cp3の出力
S403
Cp3の受理
S404
Cp3の出力
S405
Cp3の受理
S406
Cp3を検証
S407
非承認
承認
KPcp3の受理
S408
Ks1dの生成
S409
KPcp3にてKs1dを暗号化
E(KPcp3, Ks1d)の生成
S410
E(KPcp3, Ks1d)の出力
S411
E(KPcp3, Ks1d)の受理
S412
E(KPcp3, Ks1d)の出力
S413
E(KPcp3, Ks1d)の受理
S414
E(KPcp3, Ks1d)をKcp3にて復号
Ks1dの受理
S415
セッション鍵Ks2dの生成
S416
Ks2dをKs1dにて暗号化
E(Ks1d, Ks2d)の生成
S417
E(Ks1d, Ks2d)の出力
S418
E(Ks1d, Ks2d)の受理
S419
E(Ks1d, Ks2d)の出力
S420
E(Ks1d, Ks2d)の受理
S421
E(Ks1d, Ks2d)をKs1dにて復号し
Ks2dの受理
S422
対象LICの格納LBAを出力
S423
対象LICの格納LBAを受理
S424
格納LBAに対する
有効フラグ
S425
無効
有効
格納LBAに基づきLICを取得
S426
再生制限
無
ACの確認
S427
再生不可
回数制限有
格納位置のACを変更
S428
KcをKs2dにて暗号化
E(Ks2d, Kc)の生成
S429
E(Ks2d, Kc)の出力
S430
E(Ks2d, Kc)の受理
S431
E(Ks2d, Kc)の出力
S432
E(Ks2d, Kc)の受理
S433
E(Ks2d, Kc)をKs2dにて復号
Kc受理
S434
正常終了
エラー通知の出力
S435
エラー通知の受理
S436
再生拒否による終了

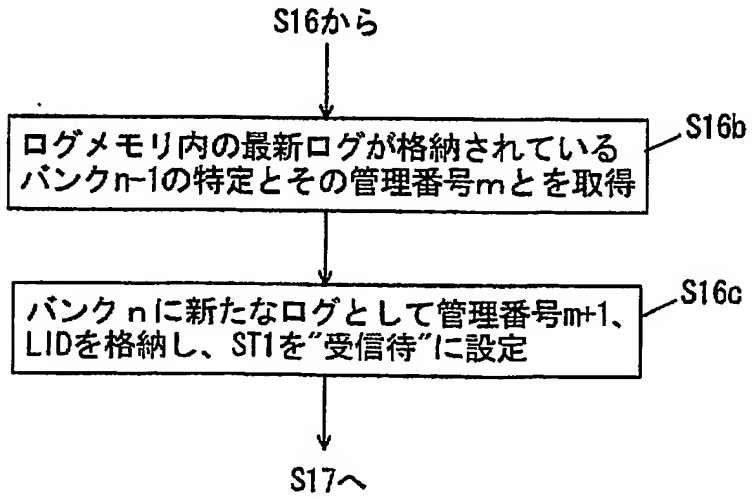
【図２５】


ライセンス提供装置 40
端末装置 10
HD 20
開始
S1
証明書の出力要求の出力
証明書の出力要求の受理
S2
Cm1の受理
S4
Cm1の出力
S3
S6
Cm1の受理
Cm1の出力
S5
S7
非承認
Cm1を検証
承認
KPcm1の受理
S8
LIDの生成
S9
ACの生成
S10
Ks1aの生成
S11
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S12
S14
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S13
LID//E(KPcm1, Ks1a)の出力
S16
LID//E(KPcm1, Ks1a)の受理
S15
S16a
ログメモリの最も古いログを格納しているバンクｎに新たなログを格納
E(KPcm1, Ks1a)をKcm1にて復号
Ks1aの受理
S17
S18
セッション鍵要求の出力
セッション鍵Ks2aの生成
S19
S201a
ログメモリのバンクｎに格納されているログにKs2aを記録
Ks2aとKPom2をKs1aにて暗号化
E(Ks1a, Ks2a//KPom2)の生成
S21
LID//E(Ks1a, Ks2a//KPom2)の出力
S22
LID//E(Ks1a, Ks2a//KPom2)の受理
S23
LID//E(Ks1a, Ks2a//KPom2)の出力
S24
再書込処理の対象
LID//E(Ks1a, Ks2a//KPom2)の受理
S25
E(Ks1a, Ks2a//KPom2)をKs1aにて復号し
Ks2aとKPom2の受理
S26
LIDおよびKcをコンテンツDBより取得
(LICの成立)
S27
LICをKPom2にて暗号化
E(KPom2, LIC)の生成
S28
E(KPom2, LIC)をKs2aにて暗号化
E(Ks2a, E(KPom2, LIC))の生成
S29
S44へ
S30へ

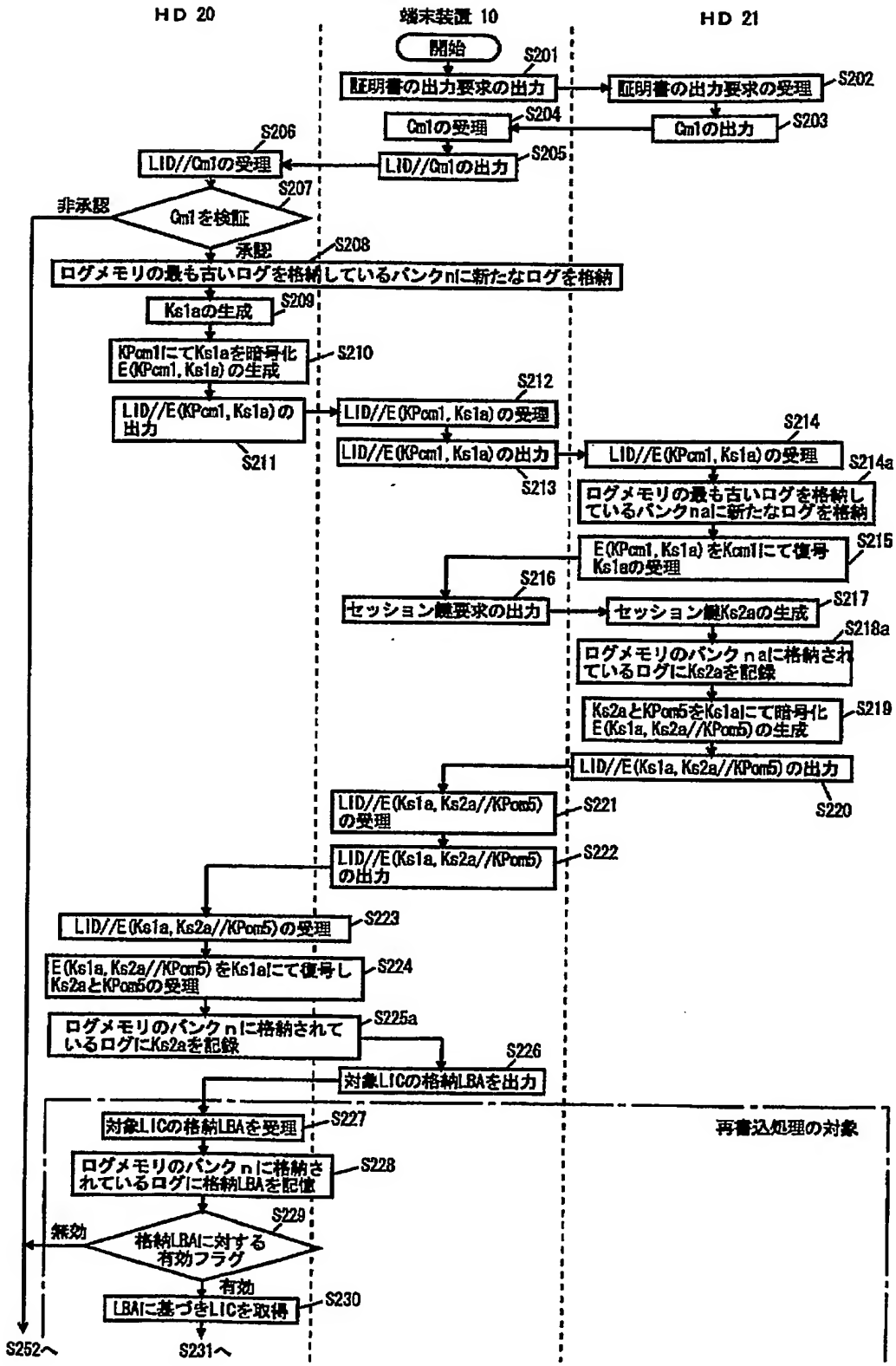
【図２６】


ライセンス提供装置 40
端末装置 10
HD 20
S7から
S29から
E(Ks2a, E(KPom2, LIC))の出力
S30
S31
E(Ks2a, E(KPom2, LIC))の受理
E(Ks2a, E(KPom2, LIC))の出力
S32
S33
E(Ks2a, E(KPom2, LIC))の受理
S34
E(Ks2a, E(KPom2, LIC))をKs2aにて復号 E(KPom2, LIC)の受理
E(KPom2, LIC)をKom2にて復号 LICの受理
S35
S36
LICを格納する格納LBAを出力
格納LBAを受理
S37
ログメモリのバンクｎに格納されているログに格納LBAを記録
S38
S39
LIDの一致
一致
不一致
S44
エラー通知の出力
S45
エラー通知の受理
エラー通知の出力
S43
書込拒否による終了
S40
格納LBAにLICを記録
再書込処理の対象
格納LBAに対する有効フラグを有効に変更
S41
S42
ログメモリのバンクｎに格納されたログのST1を"受信済"に変更
正常終了

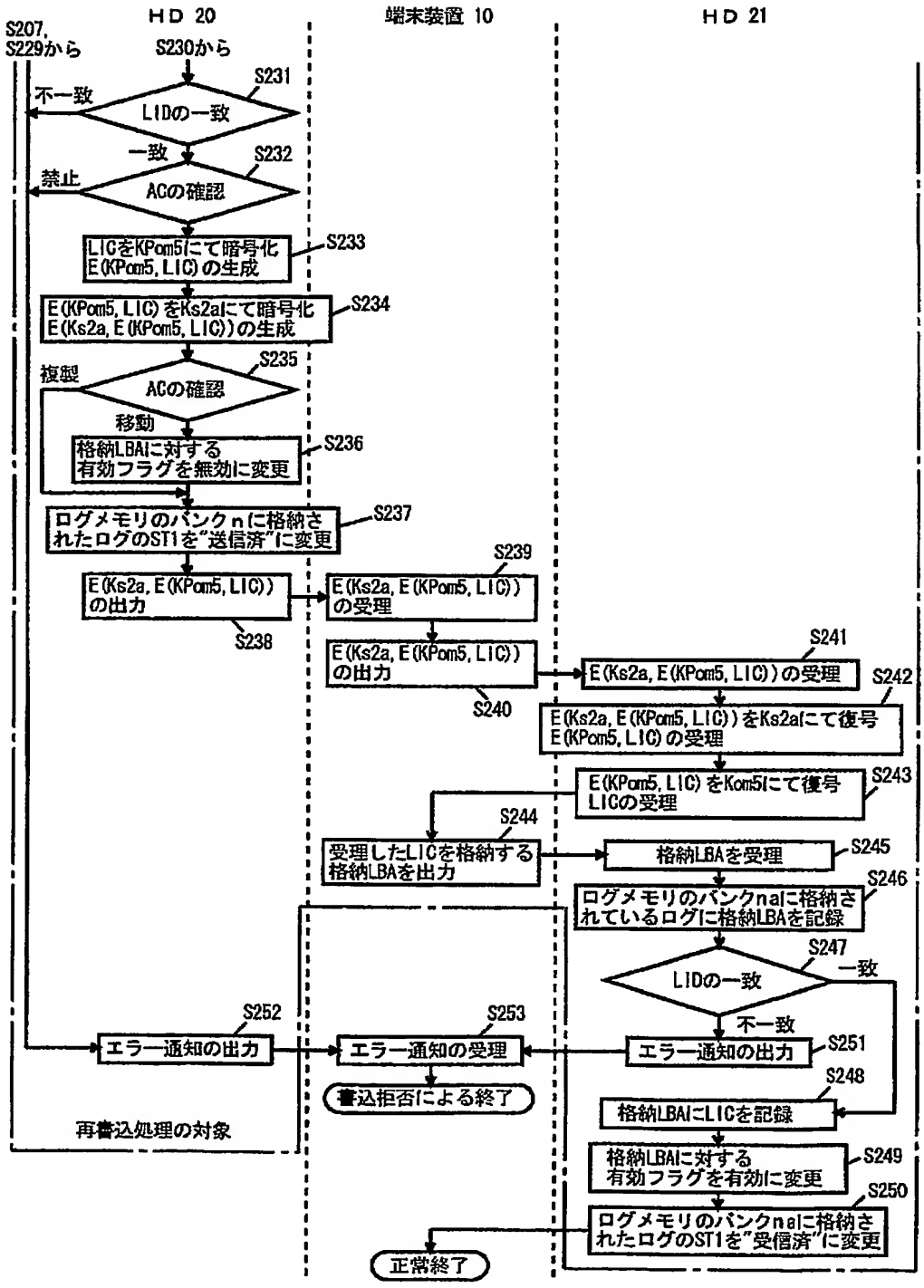
【図２７】


S16から
ログメモリ内の最新ログが格納されているバンクn-1の特定とその管理番号mとを取得
S16b
バンクｎに新たなログとして管理番号m+1、LIDを格納し、ST1を"受信待"に設定
S16c
S17へ

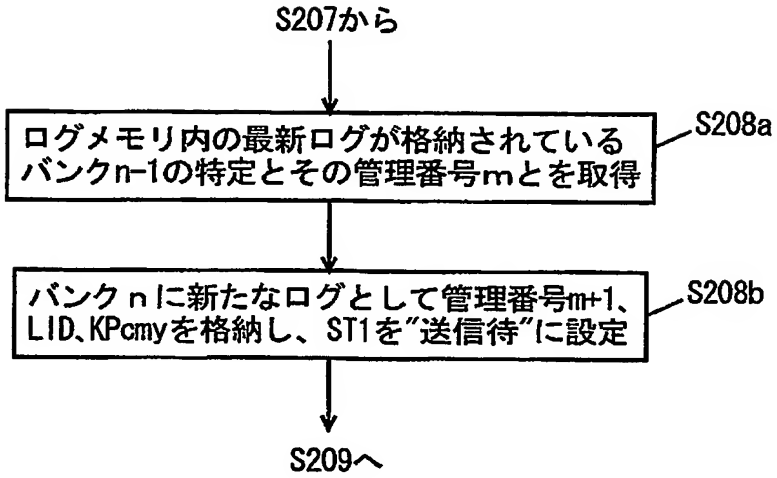
【図２８】


HD 20
端末装置 10
HD 21
開始
S201
証明書の出力要求の出力
証明書の出力要求の受理
S202
Cm1の受理
S204
Cm1の出力
S203
S206
LID//Cm1の受理
LID//Cm1の出力
S205
S207
非承認
Cm1を検証
承認
S208
ログメモリの最も古いログを格納しているバンクnに新たなログを格納
Ks1aの生成
S209
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S210
S212
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S211
LID//E(KPcm1, Ks1a)の出力
S213
S214
LID//E(KPcm1, Ks1a)の受理
S214a
ログメモリの最も古いログを格納しているバンクnaに新たなログを格納
E(KPcm1, Ks1a)をKcm1にて復号
Ks1aの受理
S215
S216
セッション鍵要求の出力
セッション鍵Ks2aの生成
S217
S218a
ログメモリのバンクnaに格納されているログにKs2aを記録
Ks2aとKPcm5をKs1aにて暗号化
E(Ks1a, Ks2a//KPcm5)の生成
S219
LID//E(Ks1a, Ks2a//KPcm5)の出力
S220
LID//E(Ks1a, Ks2a//KPcm5)の受理
S221
LID//E(Ks1a, Ks2a//KPcm5)の出力
S222
LID//E(Ks1a, Ks2a//KPcm5)の受理
S223
E(Ks1a, Ks2a//KPcm5)をKs1aにて復号しKs2aとKPcm5の受理
S224
ログメモリのバンクnに格納されているログにKs2aを記録
S225a
S226
対象LICの格納LBAを出力
対象LICの格納LBAを受理
S227
再書込処理の対象
ログメモリのバンクnに格納されているログに格納LBAを記憶
S228
S229
無効
格納LBAに対する有効フラグ
有効
LBAに基づきLICを取得
S230
S252へ
S231へ

【図２９】


HD 20
端末装置 10
HD 21
S207, S229から
S230から
S231
不一致
LIDの一致
一致
S232
禁止
ACの確認
LICをKPom5にて暗号化 E(KPom5, LIC)の生成
S233
E(KPom5, LIC)をKs2aにて暗号化 E(Ks2a, E(KPom5, LIC))の生成
S234
S235
複製
ACの確認
移動
格納LBAに対する有効フラグを無効に変更
S236
ログメモリのバンクｎに格納されたログのST1を"送信済"に変更
S237
E(Ks2a, E(KPom5, LIC))の出力
S238
S239
E(Ks2a, E(KPom5, LIC))の受理
E(Ks2a, E(KPom5, LIC))の出力
S240
S241
E(Ks2a, E(KPom5, LIC))の受理
S242
E(Ks2a, E(KPom5, LIC))をKs2aにて復号 E(KPom5, LIC)の受理
E(KPom5, LIC)をKom5にて復号 LICの受理
S243
S244
受理したLICを格納する格納LBAを出力
格納LBAを受理
S245
S246
ログメモリのバンクnaに格納されているログに格納LBAを記録
S247
LIDの一致
一致
不一致
S252
エラー通知の出力
S253
エラー通知の受理
エラー通知の出力
S251
書込拒否による終了
S248
格納LBAにLICを記録
再書込処理の対象
格納LBAに対する有効フラグを有効に変更
S249
S250
ログメモリのバンクnaに格納されたログのST1を"受信済"に変更
正常終了

【図３０】


S207から
ログメモリ内の最新ログが格納されている
バンクn-1の特定とその管理番号mとを取得
S208a
バンクｎに新たなログとして管理番号m+1、
LID、KPcmyを格納し、ST1を"送信待"に設定
S208b
S209へ

【書類名】　　要約書

【要約】

【課題】　ライセンスに対して著作権を保護し、かつ、ライセンスの送受信を再開可能とするための複数の履歴情報を重複することなく格納できるデータ記憶装置を提供する。

【解決手段】　データ記憶装置は、ログメモリ２５３を含むセキュアデータ記憶部２５０を備える。ログメモリ２５３は、複数のバンク２５３１～２５３Ｎから成り、複数のバンク２５３１～２５３Ｎにリング状に履歴情報を格納する。複数のバンク２５３１～２５３Ｎの各々は、アドレス０～Ｎ－１によって指定される。バンク２５３１～２５３Ｎの各々に格納される履歴情報は、管理番号領域２５４１と、ライセンスＩＤ（ＬＩＤ）領域２５４２と、Ｋｓ２ｘ領域２５４３と、ＳＴ１領域２５４４と、ＳＴ２領域２５４５と、ＫＰｃｍｙ領域２５４６と、ＬＢＡ領域２５４７とを含む。

【選択図】　　図７

出　願　人　履　歴　情　報

識別番号　　［０００００１８８９］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　大阪府守口市京阪本通２丁目１８番地
氏　名　　三洋電機株式会社

２．変更年月日　　１９９３年１０月２０日
［変更理由］　　住所変更
住　所　　大阪府守口市京阪本通２丁目５番５号
氏　名　　三洋電機株式会社

特願２００２－２１６７５０

出　願　人　履　歴　情　報

識別番号　　［０００００５０１６］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都目黒区目黒１丁目４番１号
氏　名　　パイオニア株式会社

出願人履歴情報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

特願２００２－２１６７５０

出　願　人　履　歴　情　報

識別番号　　［３００００１７６３６］

１．変更年月日　　２００２年　４月　４日
［変更理由］　　住所変更
住　所　　東京都千代田区丸の内１－３－１　東京銀行協会ビル１４Ｆ
氏　名　　フェニックステクノロジーズ株式会社

２．変更年月日　　２００２年　８月１６日
［変更理由］　　住所変更
住　所　　東京都新宿区新宿４－２－１８　新宿光風ビル６Ｆ
氏　名　　フェニックステクノロジーズ株式会社

３．変更年月日　　２００３年　１月　８日
［変更理由］　　住所変更
住　所　　東京都千代田区丸の内１－３－１　東京銀行協会ビル１４Ｆ
氏　名　　フェニックステクノロジーズ株式会社

特願２００２－２１６７５０

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　神奈川県川崎市中原区上小田中１０１５番地
氏　名　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社